

# Email Security Provisioning API Guide



 **GOSECURE**

© 2001–2020 GoSecure. All rights reserved. The GoSecure logo is a trademark of GoSecure, Inc. All other trademarks and registered trademarks are hereby acknowledged.

Microsoft and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Other product and company names mentioned herein may be the trademarks of their respective owners.

The GoSecure Email Security software and its documentation are copyrighted materials. Law prohibits making unauthorized copies. No part of this software or documentation may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into another language without prior permission of GoSecure.

XML 11.6

# Contents

<b>Chapter 1 API Overview</b> .....	<b>1</b>
<b>Chapter 2 Obtaining and Using an Authentication Token</b> .....	<b>2</b>
Checking the API Version Number .....	2
<b>Chapter 3 Configuration Download</b> .....	<b>4</b>
<b>Chapter 4 Configuration Upload</b> .....	<b>9</b>
<b>Chapter 5 XML Elements and Attributes</b> .....	<b>11</b>
configuration .....	11
Domain Settings .....	11
domain .....	11
categories .....	17
category .....	17
console .....	18
contentfilters .....	19
contentfilter .....	19
digest .....	20
enemies .....	21
enemy .....	21
extensions .....	21
extension .....	21
friends .....	22
friend .....	22
languages .....	22
language .....	22
properties .....	23
property .....	23
Outbound Settings .....	25
outbound .....	25
annotation .....	28
categories .....	29
category .....	29
contentfilters .....	30
contentfilter .....	30
enemies .....	30
enemy .....	30
exemptrecipients .....	31
exemptrecipient .....	31
extensions .....	31
extension .....	31
friends .....	32
friend .....	32
gateways .....	32
gateway .....	32
properties .....	33
property .....	33

tlsdomains .....	34
Group Settings .....	35
groups .....	36
group .....	36
annotation .....	39
categories .....	39
category .....	39
console .....	40
contentfilters .....	41
contentfilter .....	41
digest .....	42
enemies .....	43
enemy .....	43
exemptrecipients .....	43
exemptrecipient .....	43
extensions .....	44
extension .....	44
friends .....	44
friend .....	44
languages .....	45
language .....	45
properties .....	46
property .....	46
tlsdomains .....	47
Brand Settings .....	47
domain-defaults .....	47
outbound-defaults .....	48
Mailbox Settings .....	48
mailboxes .....	48
mailbox .....	48
alias .....	49
categories .....	49
category .....	49
console .....	50
digest .....	51
enemies .....	52
enemy .....	52
extensions .....	52
extension .....	52
friends .....	53
friend .....	53
groups .....	53
group .....	53
languages .....	54
language .....	54
properties .....	54
property .....	54
Language Codes .....	56

<b>Chapter 6 Sample XML Code</b> .....	<b>57</b>
Download Account List .....	57
Download Domain List .....	57
Viewing the Account Configuration .....	57
Adding a Domain .....	58
Deleting a Domain .....	59
Moving Domains between Accounts .....	59
Setting the User Dashboard Authentication Method .....	59
SMTP AUTH .....	59
LDAP .....	60
Assigning a Verifier to a Domain .....	60
Setting the Encryption Policy .....	60
Creating User Mailboxes .....	60
Deleting User Mailboxes .....	61
Exempting Recipients from Outbound Rate Limits .....	61
Modifying Friends and Enemies Lists .....	61
Authentication Settings .....	62
Category Filter Settings .....	62
Content Filter Settings .....	63
Digest Settings .....	63
Extension Filter Settings .....	64
Language Filter Settings .....	64
Groups .....	65
Adding a Group .....	65
Deleting a Group .....	65
Updating a Group .....	65
Assigning a Mailbox to a Group .....	65
Outbound Settings .....	66
DSN .....	66
Outbound Quarantine Access .....	66
Encryption Settings .....	66
Routing and Per-Recipient Rate Limiting .....	66
Recipient Whitelist and Authentication .....	67
<b>Chapter 7 Command Line Scripting</b> .....	<b>68</b>
Account Commands .....	68
Examples .....	69
Administrative User Commands .....	69
Creating a User .....	70
Listing Users by Role .....	70
Assigning User Administrative Roles .....	70
Revoking User Administrative Roles .....	70
Deleting an Administrative User .....	70
Quarantine Access .....	70
Retrieving a List of Messages .....	71
Retrieving a Message .....	73
Releasing a Message .....	73
Deleting a Message .....	74
Changing a Password .....	74
Domain Commands .....	74

Listing Domains .....	75
Creating a Domain .....	75
Deleting a Domain .....	76
Updating Domain Settings .....	76
Outbound IP Commands .....	76
Creating an Outbound IP .....	77
Deleting an Outbound IP .....	77
Updating an Outbound IP .....	78
Mailbox Commands .....	78
Listing Mailboxes .....	79
Creating a Mailbox .....	79
Deleting a Mailbox .....	79
Mailboxes - Update .....	80
Mailbox Alias Commands .....	80
Listing Mailbox Aliases .....	80
Creating Mailbox Aliases .....	80
Deleting a Mailbox Alias .....	81
Verifier Commands .....	81
Listing Verifiers .....	82
Creating a Verifier .....	82
Modifying a Verifier .....	82
Deleting a Verifier .....	83
Content Filter Commands .....	83
Content Filter Rules .....	84
Listing Content Filters .....	85
Downloading a Content Filter .....	85
Creating a Content Filter .....	86
Modifying a Content Filter .....	86
Deleting a Content Filter .....	86
Reporting .....	87
<b>Chapter 8 Portal API .....</b>	<b>88</b>
Token Request .....	88
Get Resellers Request .....	89
Get Reseller Details Request .....	89
Delete Reseller Request .....	90
Get Reseller Clients Request .....	90
Create Reseller Request .....	91
Edit Reseller Request .....	92
Move Client Request .....	93
Associate Client Request .....	93
<b>Appendix A Supported Time Zones .....</b>	<b>95</b>
<b>Appendix B Status Codes .....</b>	<b>102</b>

## CHAPTER 1      API Overview

The GoSecure Email Security Provisioning API helps administrators automate configuration and maintenance of system settings. It provides a scripting mechanism to batch perform such basic tasks as creating and deleting accounts, domains, and mailboxes, and customizing their properties.

The execution of this API applies to all data associated with a brand. The brand is the URL of your dashboard (either `http://my.<brand>.GoSecure.net` or `http://<brand>.GoSecure.net`). Any information in the database not specified in the XML document is left unchanged.

The Provisioning API is a REST-based XML API. Using XML syntax, data is conveyed through HTTP to the dashboard. Various command line options are available to specify the treatment of the data. A subset of the operations for manipulating configuration settings does not require the data in XML format, and can be executed with a simple HTTP request. All API calls are stateless.

API examples throughout this document use shell syntax and make use of the curl command. Curl is a command-line utility for transferring data to and from a server. It supports the following protocols: HTTP, HTTPS, FTP, FTPS, SCP, SFTP, TFTP, DICT, TELNET, LDAP or FILE.



**Note:** Executing scripts requires a system or account administrator role.

Results from API commands are wrapped in a `<result>` tag. If the return is null, the result is 0:

```
<result>0</result>
```

## CHAPTER 2 Obtaining and Using an Authentication Token

All API calls for the product require an authentication token. The return token is an opaque base64-encoded authentication token; e.g.,

YmVub2I0bUByZWZjb25kb3luY29tAAABGmV0ol-DaYnh2g9w7dVfAacwDopB1u72\_g.

Request a token from the dashboard with the following statement:

```
TOKEN=curl "http://$DASHBOARD/api/login?email=$EMAIL&password=$PASSWORD"
```

where:

Variable	Definition	Expiration	Example
DASHBOARD	Host name	7 days	my.brand.GoSecure.net
EMAIL	Email address	24 hours	admin@domain.com
PASSWORD	Password	24 hours	secret



**Note:** To use HTTPS to encrypt passwords, enable HTTPS on the appliance dashboard.

The token must be specified in every API call as a means of authentication. For example, to download the complete list of accounts, issue the following command:

```
TOKEN=curl "http://$DASHBOARD/api/account/list?token=$TOKEN"
```

Subsequent API calls using the returned token will require the user to be a System or Account Administrator.

For quarantine access commands an end user token must be used. The command for generating an end user token is:

```
TOKEN=curl "http://$DASHBOARD/api/token?token=$TOKEN&email=$USER_EMAIL"
```

### Checking the API Version Number

GoSecure strongly recommends that issuing a version check as the first part of the script when using the API. If the version does not match, the script should error out.

The Email Security API uses version numbers in the format: X.Y.

X = version - A change in X indicates a major enhancement. Backward compatibility is not guaranteed.



Y = revision - A change in Y indicates a minor enhancement. Minor enhancements retain backward compatibility.

The following command retrieves the Email Security API version number:

```
curl "http://$brand/api/version?token=$token"
```

Sample output:

```
2.6
```

## CHAPTER 3 Configuration Download

To download the complete configuration for a given domain as an XML document, enter the following statement:

```
curl "http://$DASHBOARD/api/config/download?token=$TOKEN&domain=domain.com"
```

Note that only the domain prefix needs to be specified. For example domain=GoSecure will match GoSecure.com, GoSecure.net, GoSecures.com. If no domain is specified, the resulting XML document will contain the configuration for all domains in the branded dashboard.

You can specify the configuration download version by adding the following:

```
&version=2.7>2.6
```



**Note:** In this release, for configuration download to work properly the version specified must be 2.7 or none.

The following is an example of a XML schema download:

```
<configuration version="2.7" timestamp="2013-10-29T17:12:52.493">
  <verifier name="benoit" uid="D2AAE5F3-B0F9-0AC9-3D22-F28C993EE270" account="">
    <Vrfy version="101.3807">
      <MetaData>
        <Editable>true</Editable>
      </MetaData>
      <LDAP defaults="ActiveDirectory">
        <Host secure="false">postal.GoSecure.com</Host>
        <HostListOrder>Shuffle</HostListOrder>
        <Timeout>5</Timeout>
      </LDAP>
    </Vrfy>
  </verifier>
  <domain-defaults gateway="mail.GoSecure.com" clienttls="none" emailcontinuity="false"
inboundTLSDomains="" authenticator="" dsnunrestricted="false" maxmsgsize="5" spoolerduration="96"
senderSpooof="false" antiSpooof="" retainblocked="false" retaindelivered="true" mbcleanup="3"
token="true" balanced="false" discovery="disabled" unrecognized="bounce" odi="true"
notifydiscovery="true" sessionverify="false" dhaprotection="bounce_only">
  <contentfilters/>
  <console enabled="true" quarantine="true" outbound="false" release="true" settings="true"
policies="true" foreign="true" attachments="true" sender="true"/>
</domain-defaults>
  <outbound-defaults gateway="" clienttls="available" authenticator="" dsnunrestricted="false"
maxmsgsize="unlimited" spoolerduration="2" retainblocked="false" retaindelivered="false"
mphuser="unlimited" mphother="unlimited" mphuserresponse="451 Hourly outbound rate limit
exceeded" mphotherresponse="550 Hourly outbound rate limit exceeded" rcptlimit="unlimited"
rcptlimitresponse="451 Recipient limit exceeded for this sender" dsn="false" dsnlimit="3"
sessiontls="available" annotation="none">
  <contentfilters/>
```

```

<exemptrecipients/>
<tlsdomains policy="available"/>
<gateways/>
</outbound-defaults>
<groups>
  <group name="SVT Group 2" uid="23a6ef94-0589-4e4e-abf6-f8321da7085a" domainname="example.com"
    grouppriority="2" type="outbound" gateway="encryption.example.com" timezone="" bcc="">
    <annotation/>
    <friends/>
    <enemies/>
    <categories/>
    <languages/>
    <extensions/>
    <console enabled="" quarantine="" outbound="" release="" settings="" policies="" foreign=""
      attachments="" sender=""/>
  </group>
  <group name="SVT Group 2" uid="9d7a4b1c-9502-40e1-99b8-5e457d721930" domainname="example.com"
    grouppriority="3" type="inbound" gateway="mail2.example.com" timezone="" bcc="">
    <annotation/>
    <digest detail="inherit" format="inherit" language="inherit" frequency="inherit" order=""/>
    <friends/>
    <enemies/>
    <categories/>
    <languages/>
    <extensions/>
    <console enabled="" quarantine="" outbound="" release="" settings="" policies="" foreign=""
      attachments="" sender=""/>
  </group>
</groups>
<contentfilter name="Bad Words" uid="86B88D3C-F29B-6F59-6B0E-6C26603FC18B" account="A5A659B3-6901-
4D8A-B231-100C0DF2FCC0"> [{"parts":["HEADER","TEXT"],"filters":["bar","foo"], "headers":
["Subject:","From:"]} ]
</contentfilter>
<contentfilter name="Another List" uid="BFE78762-1788-4DA2-B84F-3C73D3C7EF09" account="A5A659B3-
6901-4D8A-B231-100C0DF2FCC0"> [{"parts":["HEADER"],"filters":["badword0","badword1"], "headers":
["Subject:","Sender:"]} ]
</contentfilter>
<domain name="example.com" notifydiscovery="true" account="C2F26595-29E2-764D-3519-13"
emailcontinuity="false" inboundTLSDomains="" timezone="" gateway="" discovery="external"
authenticator="" unrecognized="discard" dsn="false" dsnlimit="0" dsnunrestricted="false"
maxmsgsize="5" odi="false" verifier="D2AAE5F3-B0F9-0AC9-3D22-F28C993EE270" outboundaccess="false"
consoleaccess="true" clienttls="none" dhaprotection="bounce_only" bcc="b5e91e4a-40f6-12df-9e06-
12313b001843@mail.gosecurearchive.com" balanced="false" spoolerduration="96" senderSpoof="false"
antiSpoof="" emcAutoEnabled="false" emcAutoEnableDuration="15" emcautodisableduration="900000"
emctestemail="" emcautodisabled="false" emcOfflineTimeout="600000"emconlinetimeout="600000">
  <digest detail="red" format="html" frequency="never" order="Date-"/>
  <categories>
    <category name="junk" action="quarantine"/>
    <category name="virus" action="quarantine"/>
    <category name="adult" action="quarantine"/>
    <category name="spam" action="quarantine"/>
  </categories>
  <languages/>
  <extensions>
    <extension name="asd" action="quarantine"/>
    <extension name="bat" action="quarantine"/>
    <extension name="cab" action="quarantine"/>
    <extension name="chm" action="quarantine"/>
    <extension name="com" action="quarantine"/>

```

```

<extension name="cpl" action="quarantine"/>
<extension name="dat" action="quarantine"/>
<extension name="dll" action="quarantine"/>
<extension name="eml" action="quarantine"/>
<extension name="exe" action="quarantine"/>
<extension name="hlp" action="quarantine"/>
<extension name="hta" action="quarantine"/>
<extension name="inf" action="quarantine"/>
<extension name="lnk" action="quarantine"/>
<extension name="msi" action="quarantine"/>
<extension name="msp" action="quarantine"/>
<extension name="nws" action="quarantine"/>
<extension name="ocx" action="quarantine"/>
<extension name="pif" action="quarantine"/>
<extension name="reg" action="quarantine"/>
<extension name="scr" action="quarantine"/>
<extension name="sct" action="quarantine"/>
<extension name="shb" action="quarantine"/>
<extension name="shs" action="quarantine"/>
<extension name="vbe" action="quarantine"/>
<extension name="vbs" action="quarantine"/>
<extension name="vcd" action="quarantine"/>
<extension name="vcf" action="quarantine"/>
<extension name="wsc" action="quarantine"/>
<extension name="wsf" action="quarantine"/>
<extension name="wsh" action="quarantine"/>
<extension name="zip" action="quarantine"/>
</extensions>
<contentfilters>
  <contentfilter uid="86B88D3C-F29B-6F59-6B0E-6C26603FC18B" action="quarantine"/>
  <contentfilter uid="BFE78762-1788-4DA2-B84F-3C73D3C7EF09" action="quarantine"/>
</contentfilters>
<console enabled="true" quarantine="true" outbound="false" release="true" settings="true"
policies="true" foreign="true" attachments="true" sender="true"/>
<mailbox name="admin" status="active" consoleaccess="" timezone="" bcc="">
  <digest detail="inherit" format="inherit" frequency="inherit" order="Date-"/>
  <categories/>
  <languages/>
  <extensions/>
</mailbox>
<mailbox name="alex" status="active" consoleaccess="" timezone="" bcc="">
  <digest detail="inherit" format="inherit" frequency="inherit" order="Date-"/> <categories/>
  <languages/> <extensions/>
  <groups> <group type="manual">SVT Group 2</group> <group type="auto">engineering</group>
  <group type="auto">sales</group> </groups>
</mailbox>
<mailbox name="chris" status="active" consoleaccess="" timezone="" bcc="">
  <digest detail="red" format="html" frequency="daily" order="Date+"/>
  <categories>
    <category name="junk" action="quarantine"/>
    <category name="virus" action="quarantine"/>
    <category name="phish" action="quarantine"/>
    <category name="adult" action="quarantine"/>
    <category name="spam" action="quarantine"/>
  </categories>
  <languages>
    <language name="BS" action="markup" markup="FOREIGN:"/>
    <language name="CC" action="quarantine"/>
    <language name="CE" action="quarantine"/>
    <language name="CY" action="quarantine"/>

```

```

    <language name="EE" action="quarantine"/>
    <language name="NO" action="quarantine"/>
    <language name="SE" action="quarantine"/>
    <language name="ar" action="quarantine"/>
    <language name="el" action="quarantine"/>
    <language name="he" action="quarantine"/>
    <language name="ja" action="quarantine"/>
    <language name="ko" action="quarantine"/>
    <language name="th" action="quarantine"/>
    <language name="tr" action="quarantine"/>
    <language name="zh" action="quarantine"/>
  </languages>
  <extensions>
    <extension name="asd" action="quarantine"/>
    <extension name="bat" action="quarantine"/>
    <extension name="cab" action="quarantine"/>
    <extension name="chm" action="quarantine"/>
    <extension name="com" action="quarantine"/>
    <extension name="cpl" action="quarantine"/>
    <extension name="dat" action="quarantine"/>
    <extension name="dll" action="quarantine"/>
    <extension name="eml" action="quarantine"/>
    <extension name="exe" action="quarantine"/>
    <extension name="hlp" action="quarantine"/>
    <extension name="hta" action="quarantine"/>
    <extension name="inf" action="quarantine"/>
    <extension name="lnk" action="quarantine"/>
    <extension name="msi" action="quarantine"/>
    <extension name="msp" action="quarantine"/>
    <extension name="nws" action="quarantine"/>
    <extension name="ocx" action="quarantine"/>
    <extension name="reg" action="quarantine"/>
    <extension name="sct" action="quarantine"/>
    <extension name="shb" action="quarantine"/>
    <extension name="shs" action="quarantine"/>
    <extension name="vbe" action="quarantine"/>
    <extension name="vbs" action="quarantine"/>
    <extension name="vcd" action="quarantine"/>
    <extension name="vcf" action="quarantine"/>
    <extension name="wsc" action="quarantine"/>
    <extension name="wsf" action="quarantine"/>
    <extension name="wsh" action="quarantine"/>
    <extension name="zip" action="quarantine"/>
  </extensions>
  <alias name="christopher"/>
</mailbox>
<mailbox name="hawaii_mom" status="active" failure="2009-07-31T22:19:27.644" consoleaccess=""
timezone="" bcc="">
  <digest detail="inherit" format="inherit" frequency="inherit" order=""/>
  <categories/>
  <languages/>
  <extensions/>
</mailbox>
<mailbox name="test" status="inactive"/>
</domain>
<outbound source="1.2.3.4/32" account="a5a659b3-6901-4d8a-b231-100c0df2fcc0" timezone="" bcc=""
gateway="" authenticator="" dsn="true" dsnlimit="unlimited" dsnunrestricted="true"
maxmsgsize="100" spoolerduration="1" retainblocked="true" authrequired="true" mphuser="unlimited"
mphother="unlimited" mphuserresponse="451 Hourly outbound rate limit exceeded"

```

```

mphotoresponse="550 Hourly outbound rate limit exceeded" rcptlimit="unlimited"
rcptlimitresponse="451 Recipient limit exceeded for this sender" sessiontls="none"
annotation="append">
<friends/>
<enemies/>
<categories>
  <category name="credit" action="markup" markup="CREDIT CARD:"/>
  <category name="ssn" action="markup" markup="SOCIAL SECURITY:"/>
  <category name="virus" action="quarantine"/>
  <category name="phish" action="quarantine"/>
  <category name="adult" action="quarantine"/>
  <category name="pdf" action="quarantine"/>
  <category name="bot" action="quarantine"/>
  <category name="spam" action="quarantine"/>
</categories>
<languages/>
<extensions>
  <extension name="asd" action="quarantine"/>
  <extension name="bat" action="block"/>
  <extension name="cab" action="quarantine"/>
  <extension name="chm" action="quarantine"/>
  <extension name="com" action="block"/>
  <extension name="cpl" action="quarantine"/>
  <extension name="dll" action="quarantine"/>
  <extension name="exe" action="quarantine"/>
  <extension name="hlp" action="quarantine"/>
  <extension name="hta" action="quarantine"/>
  <extension name="inf" action="quarantine"/>
  <extension name="lnk" action="quarantine"/>
  <extension name="msi" action="quarantine"/>
  <extension name="msp" action="quarantine"/>
  <extension name="nws" action="quarantine"/>
  <extension name="ocx" action="quarantine"/>
  <extension name="pif" action="block"/>
  <extension name="reg" action="quarantine"/>
  <extension name="scr" action="block"/>
  <extension name="sct" action="quarantine"/>
  <extension name="shb" action="quarantine"/>
  <extension name="shs" action="quarantine"/>
  <extension name="vbe" action="quarantine"/>
  <extension name="vbs" action="quarantine"/>
  <extension name="wsc" action="quarantine"/>
  <extension name="wsf" action="quarantine"/>
  <extension name="wsh" action="quarantine"/>
</extensions>
<contentfilters>
  <contentfilter uid="52bd2714-a881-4772-acf2-efb82cf53bd7" action="quarantine"/>
</contentfilters>
<exemptrecipients/>
<tlsdomains policy="none"/>
<gateways/>
<annotation>
  <p>Test Annotation message - xxxyyyyzzz</p>
</annotation>
</outbound>
</configuration>

```

## CHAPTER 4 Configuration Upload

Upload XML formatted data to the dashboard to modify your system configuration settings. The data can be uploaded in a file or submitted through a POST command.

The following upload API call takes as input the same schema as described in [Configuration Download](#) in the file `domain.xml`:

```
curl -F "data=@domain.xml"  
"http://$DASHBOARD/api/config/upload?token=$TOKEN&account=$ACCOUNT&update=true"
```

The data can also be uploaded using the POST command:

```
curl -X POST -H 'Content-type: text/xml' -d '<xml data>'  
"http://$DASHBOARD/api/config/upload?token=$TOKEN&account=$ACCOUNT&update=true"
```



**Note:** Enter the above command on a single line. It cannot work with a new line in the xml data. The length of the command will be limited by the operating system. The xml data content can be within double quotes if quotes within the data are escaped.

Where `$TOKEN` is the authentication token retrieved with the login command and `$ACCOUNT` is the UID of the account.

To get a list of UIDs for all accounts, enter the following statement:

```
curl "http://$DASHBOARD/api/account/list?token=$TOKEN"
```

To get a subset of the accounts on the server, enter the following statement:

```
curl "http://$DASHBOARD/api/account/list?token=$TOKEN&name=ad"
```

This will return the list of accounts starting with the string "ad".

The following optional parameters can be specified as part of the URL:

Parameter	Description	Valid Options
-----------	-------------	---------------

update	Whether or not to update the existing configuration. If this parameter is false or not specified, no modifications are performed on the database.	<b>true:</b> The database is updated with any new or modified information in the XML document, and the resulting XML document will describe what actions were taken. <b>false:</b> The database is not updated
force	This parameter has been deprecated. It no longer has any affect.	
delete	Specifies whether or not to delete mailboxes, domains, or aliases not specified in the XML document. When true, any mailbox or alias not specified in the configuration XML will be deleted from the system. This option should only be used when the supplied XML configuration is complete and authoritative. <b>Note:</b> Use the true option carefully.	<b>true:</b> All elements in the database not specified in the XML document will be deleted. <b>false:</b> No changes are made to items not specified in the XML document.
account	The account that the API will act upon. Domains cannot be created unless a valid active account is specified.	The UID of the account to use when creating new domains. See the example above.

**Notes:**

New domains cannot be added to the system unless a valid active account is specified.

When an Account UID is specified in the config upload http request all of the objects in the XML file must be in that Account. Otherwise, the system interprets the request as a move of those objects to that Account.



## CHAPTER 5 XML Elements and Attributes

The following sections show the supported XML API elements, attributes, their descriptions, and valid options. Required elements and attributes are noted.



**Note:** All elements, attributes, and values are case-sensitive.

### configuration

<configuration> : Root element.

Attribute	Description	Valid Options
version	The version of the configuration schema. Version is returned with the download and is ignored when uploading.	2.7
timestamp	The GMT date and time that the XML document was produced.	

### Domain Settings

When creating a domain, elements and attributes not specified derive their values from system level defaults. On domain updates, an element or attribute not specified is not changed. The following sections show domain-level elements and tables with their attributes. Note that all attributes are optional unless specified as required.

#### domain

<domain> : The child element of <configuration>.

There can be only one <domain> element per domain. If there are multiple entries, the last entry is used.

Attribute	Description	Valid Options
name	The name of the domain. (Required)	Fully qualified domain name.

Attribute	Description	Valid Options
outbound (read-only)	Specifies that this is an outbound IP. It only appears when an outbound IP is defined. <b>Note:</b> This attribute will be deprecated in a future release. See <a href="#">Outbound Settings</a> for elements and attributes for outbound IPs.	<b>true:</b> The element is an outbound IP.
gateway	Comma separated list of the domain gateways.	Mail server.
clienttls	Encryption setting between the product and the mail gateway.	<b>none:</b> Encryption never offered during the session. <b>available:</b> If an encrypted session cannot be established, the message is sent in the clear. <b>required:</b> If an encrypted session can not be established then the connection is closed <b>valid:</b> The certificate must be valid. <b>trusted:</b> The certificate must be trusted.

Attribute	Description	Valid Options
discovery	The method for discovering new mailboxes for the domain.	<p><b>automatic:</b> Creates a mailbox after more than one message is received within a set time period.</p> <p><b>disabled:</b> No level of automation, you must manually enter and delete mailboxes as needed.</p> <p><b>vfry:</b> Uses the SMTP VRFY command to validate mailbox addresses on the domain's mail gateway. If the mailbox does not exist, it creates it. A valid VRFY response is 250.</p> <p><b>rcpt:</b> Uses the SMTP RCPT TO command to validate mailbox addresses on the domain's mail gateway. If the mailbox does not exist, it creates it. A valid response is 250.</p> <p><b>external:</b> Uses a previously defined verifier.</p> <p><b>&lt;domain_name&gt;</b> : Mail sent to unrecognized recipients is rewritten to this domain. The message is handled as if it was sent to the rewritten address.</p>
notifydiscovery	The attribute on the domain that controls the creation of mailboxes on discovery.	<p><b>true:</b> mailbox created</p> <p><b>false:</b> mailbox not created</p>
unrecognized	The method for handling a message to an unknown user when the mailbox discovery is set to disabled.	<p><b>accept:</b> Forward message to customer's mail server without spam/virus filtering.</p> <p><b>bounce:</b> Return to sender with standard 550 unrecognized recipient.</p> <p><b>discard:</b> Deletes without sending notification.</p> <p><b>forward email address:</b> Mail is sent to specified email address, such as your mail administrator. This email address does not have to be in a domain in the Email Security system.</p>

Attribute	Description	Valid Options
odi	The method for handling mailbox aliases when forwarding to the mail gateway.	<b>true:</b> Preserves the mailbox alias before sending the message to the mail gateway. <b>false:</b> Rewrites the alias with the primary SMTP address.
mbcleanup	Automatically remove invalid mailboxes after specified number of days.	Integer greater than or equal to 3.
maxmsgsize	The maximum size of an individual message. Measured in megabytes. Messages of a size greater than the defined maximum are rejected by the mail server.	Integer from 1 through 100.
timezone	Time zone of the domain.	See <a href="#">Supported Time Zones</a> for a list of supported time zones.
authenticator	Verifier used for dashboard authentication. Supports both inbound and outbound traffic.	UID of the custom LDAP authenticator.
verifier	Verifier to be used for mailbox discovery.	UID of the verifier.
delete	Deletes the domain.	<b>true:</b> Deletes the domain.
bcc	Sends a copy of every delivered message to this archive collection address.	Email address.
account	Moves the domain from the existing account to the specified account.	UID of the account to move the domain to.
emailcontinuity	Enables Email Continuity for the domain. <b>Note:</b> Email Continuity must be licensed for this setting to have an effect.	<b>true:</b> Email Continuity is enabled. <b>false:</b> Email Continuity is disabled.

Attribute	Description	Valid Options
emcAutoEnabled	Whether to enable automatic Email Continuity.	<b>true</b> : Email Continuity will be enabled automatically. <b>false</b> : Email Continuity must be enabled manually.
emcAutoEnableDuration	The amount of time in milliseconds for the mail server to be unreachable before Email Continuity is automatically turned on.	Integer
emcAutoDisabled	Turn on/off automatic disabling of Email Continuity.	<b>true</b> : Email Continuity will be disabled automatically. <b>false</b> : Email Continuity must be disabled manually.
emcAutoDisableDuration	The amount of time in milliseconds for the mail server to be reachable before Email Continuity is automatically turned off.	Integer
emcofflinetimeout	The amount of time in milliseconds after Email Continuity has been turned off until it can be automatically enabled again.	Integer
emconlinetimeout	The amount of time in milliseconds after Email Continuity has been turned on until it can be automatically disabled again.	Integer
emctestemail	Address for sending a test email when the mail server is down.	Email address.

Attribute	Description	Valid Options
spoolerduration	Maximum amount of time in hours that mail will be stored (spooled) on the system before it is bounced back to the sender in the event of mail server failure.	Integer from 1 through 320
balanced	How mail is distributed when multiple mail gateways are configured.	<b>false:</b> Mail is sent to the first entered server. If the server is unavailable, mail goes to the second server, and so on. <b>true:</b> Mail is evenly distributed between all configured servers.
outboundaccess	Domain-level command that enables or disables access to quarantined outbound messages from the user's Personal Dashboard.	<b>true:</b> Allows access to outbound filtered messages through the user's Personal Dashboard. <b>false:</b> Disallows access to outbound filtered messages through the user's Personal Dashboard.
consoleaccess	Determines whether user has access to the dashboard and receives the digest.	<b>true:</b> Allows access to the user's Personal Dashboard and Spam Digest. <b>false:</b> Disallows access to the user's Personal Dashboard and Spam Digest.
dhaprotection	Sets level of Directory Harvest Attack (DHA) protection.	<b>reject_only:</b> All unrecognized recipients are rejected with 550 Rejected. <b>reject_preference:</b> Some unrecognized recipients are accepted for filtering and possible bounce (if not spam). <b>bounce_preference:</b> Most unrecognized recipients are accepted for filtering and possible bounce (if not spam). <b>bounce_only:</b> All unrecognized recipients are accepted for filtering and possible bounce (if not spam).

Attribute	Description	Valid Options
retaindelivered	Attribute for keeping legitimate mail.	true or false
retainblocked	Attribute for handling blocked mail.	<b>true</b> : Blocked mail is kept in the administrative quarantine. <b>false</b> (default): Blocked mail is deleted.
disableImageLinks	Disables links for images in delivered mail.	<b>true</b> : Image links are converted to plain text. <b>false</b> : Image links are "live."
disableURLS	Disables web links in delivered mail.	<b>true</b> : Web links are converted to plain text. <b>false</b> : Web links are "live."
inboundTLSdomains	Specifies domains that must use TLS.	Comma separated list of domains that are required to use TLS when they send mail to the domain.
antiSpooF	Enables general spoof protection.	Comma separated list of IP addresses and email addresses that are exceptions. <b>127.0.0.1</b> : Turn general spoof protection on/off without including any exceptions.
senderSpooF	Enable/disable smart anti-spoof protection.	true or false
token	Allows auto-login from the digest when set to true.	<b>true</b> : User can click the link in the digest to the Personal Dashboard and be automatically logged in. <b>false</b> : Clicking the link in the digest takes the user to the Personal Dashboard, but a login is required.

### categories

<categories> : Child element of <domain>.

### category

<category> : Child element of <categories> and <domain>.

Use the <category> element to add or update a specific category. To specify the complete and authoritative set of category-based delivery policies, enclose one or more <category> elements in a <categories> element. Using the <categories> element overrides the existing defaults.

Attribute	Description	Valid Options
name	Message type. (Required)	Virus, adult, phish, bot, spam, pdf, macro, junk, credit, ssn, unscanned.
action	The delivery option for mail in the category. If no action is specified, the category is removed. (Required)	<p><b>allow:</b> Allows the mail to pass to the user's mailbox.</p> <p><b>markup:</b> Allows the mail to pass to the user's mailbox with prepended text in the subject line. The markup prefix is specified using the markup attribute.</p> <p><b>strip:</b> Strips (permanently deletes) the attachment and delivers the message with an annotation specifying how many attachments were stripped.</p> <p><b>quarantine:</b> Sends the mail to the quarantine.</p> <p><b>block:</b> Deletes the mail.</p>
markup	Text string prepended to the subject line of marked up mail. (Required if action is markup.)	Up to 50 alphanumeric characters.

## console

<console> : Child element of <domain>.

Attribute	Description	Valid Options
enabled	If false, the console will not be available to users in this domain.	true or false
quarantine	If false, users will not have access to their personal quarantine.	true or false
outbound	If false, users will not have access to their outbound quarantine.	true or false



Attribute	Description	Valid Options
settings	If false, users will not be able to change settings (such as digest settings, time zone, etc.).	true or false
policies	If false, users will not be able to change disposition policies for messages based on category.	true or false
foreign	If false, users will not be able to change disposition policies based on languages (i.e., character sets).	true or false
attachments	If false, users will not be able to change dispositions based on attachment file extensions.	true or false
sender	If false, users will not be able to change dispositions based on senders such as friends/enemies list.	true or false
release	If false, users cannot release inbound mail from the quarantine.	true or false
outboundRelease	If false, users cannot release outbound mail from the quarantine.	true or false
dlprelease	If false, users cannot release DLP messages from the quarantine.	true or false
messagedelete	If false, users cannot delete messages from the quarantine.	true or false

### contentfilters

<contentfilters> : Child element of <domain>.

### contentfilter

<contentfilter> : Child element of <contentfilters> and <domain>.

Use the <contentfilter> element to add or update a specific content filter. To specify the complete and authoritative set of content filter-based delivery policies, enclose the <contentfilter> elements in a <contentfilters> element.

Attribute	Description	Valid Options
uid	UID of the content filter. (Required)	GUID of a content filter.
action	Action to take on the content filter. If no action is specified, the content filter is removed. (Required)	<b>allow</b> : Allows the mail to pass to the user's mailbox. <b>markup</b> : Allows the mail to pass to the user's mailbox with prepended text in the subject line. The markup prefix is specified using the markup attribute. <b>quarantine</b> : Sends the mail to the quarantine. <b>block</b> : Deletes the mail.
markup	Text string to prepend the subject line of marked up text. (Required if action is markup.)	Text string.

## digest

<digest> : Child element of <domain>.

Attribute	Description	Valid Options
detail	Controls the (minimum) level of detail on the digest. (At least one attribute required.)	<b>summary</b> : Summary only. <b>green</b> : Displays only mail from the green zone (junk). <b>yellow</b> : Displays mail from the yellow zone (foreign, attachments) plus mail from the green zone. <b>red</b> : Displays all mail in the quarantine.
format	Format of the daily digest. (At least one attribute required.)	Text, html, or multipart.
frequency	The delivery frequency of the digest. (At least one attribute required.)	<b>never</b> : The digest is not sent. <b>daily</b> : The digest is sent every day. <b>weekly</b> : The digest is sent once a week.
order	The order the messages in the digest are sorted. (At least one attribute required.)	<b>Date-</b> : Sorts from newest to oldest. <b>Date+</b> : Sorts from oldest to newest. <b>Size-</b> : Sorts from largest to smallest. <b>Size+</b> : Sorts from smallest to largest.

Attribute	Description	Valid Options
		<b>Mailbox:</b> Sorts on the "SMTP Mail From" field. <b>Sender:</b> Sorts on the "From" field in the Mime Header. <b>Subject:</b> Sorts by subject.

## enemies

<enemies> : Child element of <domain>.

## enemy

<enemy> : Child element of <enemies> and <domain>.

Use the <enemy> element to add or update an individual non-trusted mail source to automatically quarantine. To specify the complete and authoritative list of enemies, enclose the <enemy> elements in an <enemies> element. Using the <enemies> element overrides the existing enemies list.

Attribute	Description	Valid Options
name	Name of email address to quarantine.	Email address, domain, IP address, country code.
delete	Optional attribute to delete a name from the list.	<b>true:</b> Deletes the name from the list. <b>false:</b> Does not delete the name from the list.

## extensions

<extensions> : Child element of <domain>.

## extension

<extension> : Child element of <extensions> and <domain>.

Use the <extension> element to add or update a specific extension. To specify the complete and authoritative set of extension-based delivery policies, enclose the <extension> elements in an <extensions> element. Using the <extensions> element overrides the existing defaults.

Attribute	Description	Valid Options
name	File extension. (Required)	<b>Note:</b> The "." should not be specified.

Attribute	Description	Valid Options
action	Action to take on file extensions of attached messages. If no action is specified, the extension is removed. (Required)	<b>allow</b> : Allows the mail to pass to the user's mailbox. <b>markup</b> : Allows the mail to pass to the user's mailbox with prepended text in the subject line. The markup prefix is specified using the markup attribute. <b>quarantine</b> : Sends the mail to the quarantine. <b>block</b> : Deletes the mail.
markup	Text string to prepend the subject line of marked up text. (Required if action is markup.)	

**friends**

<friends> : Child element of <domain>.

**friend**

<friend> : Child element of <friends> and <domain>.

Use the <friend> element to add or update an individual trusted mail source. To specify the complete and authoritative list of friends, enclose the <friend> element in a <friends> element. Using the <friends> element overrides the existing friends list.

Attribute	Description	Valid Options
name	Messages from this sender won't be filtered.	Email address, domain, IP address, country code.
delete	Optional attribute to delete a name from the list.	<b>true</b> : Deletes the name from the list. <b>false</b> : Does not delete the name from the list.

**languages**

<languages> : Child element of <domain>.

**language**

<language> : Child element of <languages> and <domain>.

Use the <language> element to add or update a specific language. To specify the complete and authoritative set of language-based delivery policies, enclose the <language> elements in a <languages> element. Using the <languages> element overrides the existing defaults.

Attribute	Description	Valid Options
name	Character set name. (Required)	See <a href="#">Language Codes</a> for the list of supported languages.
action	Action to take on messages in selected language. If no action is specified, the language is removed. (Required)	<b>allow</b> : Allows the mail to pass to the user's mailbox. <b>markup</b> : Allows the mail to pass to the user's mailbox with prepended text in the subject line. The markup prefix is specified using the markup attribute. <b>quarantine</b> : Sends the mail to the quarantine. <b>block</b> : Deletes the mail.
markup	Text string prepended to the subject line of marked up mail. (Required if action is markup.)	Up to 50 alphanumeric characters.

### properties

<properties> : Child element of <domain>.

### property

<property> : Child element of <properties> and <domain>.

Use the <property> element to add or update authentication specifications. To specify the complete and authoritative set of language-based delivery policies, enclose the <property> elements in a <properties> element. Using the <properties> element overrides the existing defaults.

Attribute	Description	Valid Options
captchaLimit	The number of failed login attempts that generates a captcha challenge.	Positive integer.

Attribute	Description	Valid Options
enemyAction	How blacklist entries will be handled.	<b>quarantine:</b> Messages are saved in the quarantine for review. <b>block:</b> Messages are deleted immediately.
includeOutbound	Whether outbound messages are included in the spam digest.	<b>true:</b> The spam digest includes outbound messages. <b>false:</b> The spam digest does not include outbound messages.
passwordExpiration	The number of days between required user password resets.	Positive integer.
passwordLength	The number of characters required for a valid password.	Positive integer.
passwordLower	Whether the password requires a lowercase character.	<b>true:</b> The password must contain at least one lowercase character. <b>false:</b> The password does not require a lowercase character.
passwordNumber	Whether the password requires a number.	<b>true:</b> The password must contain at least one number. <b>false:</b> The password does not require a number.
passwordSpace	Whether the password requires a space.	<b>true:</b> The password must contain at least one space. <b>false:</b> The password does not require a space.
passwordSpecial	Whether the password requires a special (non-alphanumeric) character.	<b>true:</b> The password must contain at least one special character. <b>false:</b> The password does not require a special character.

Attribute	Description	Valid Options
passwordUpper	Whether the password requires a uppercase character.	<b>true:</b> The password must contain at least one uppercase character. <b>false:</b> The password does not require a uppercase character.
sessionTimeout	The number of minutes before the dashboard returns to the login screen.	Positive integer.
viewSpfExceptions	Allows the user to exempt domains from SPF handling.	<b>true:</b> User can set SPF exceptions. <b>false:</b> User cannot set SPF exceptions.
fuzzAction	Filters messages similar to the filtered domain (for example, yourdomain.com would include youdomain.com).	<b>allow:</b> Allows the mail to pass to the user's mailbox. <b>markup:</b> Allows the mail to pass to the user's mailbox with prepended text in the subject line. The markup prefix is specified using the markup attribute. <b>quarantine:</b> Sends the mail to the quarantine.
annotationHeader	Defines a custom email header that will be added to all incoming messages for the domain.	Email header is defined as header:value. Example: <property key="annotationHeader">mailtest:true</property>

## Outbound Settings

When setting up an outbound IP, elements and attributes not specified derive their values from system level defaults. On update, an element or attribute not specified is not changed. The following sections show outbound IP elements and tables with their attributes. Note that all attributes are optional unless specified as required.

### outbound

<outbound> : The child element of <configuration>.

There can be only one <outbound> element per outbound IP. If there are multiple entries, the last entry is used.

Attribute	Description	Valid Options
source	The outbound IP address. (Required)	IP address in CIDR notation.
maxmsgsize	The maximum size of an individual message. Measured in megabytes. Messages of a size greater than the defined maximum are rejected by the mail server.	Integer from 1 through 100.
timezone	Time zone of the outbound IP address.	See <a href="#">Supported Time Zones</a> for a list of supported time zones.
authserver	Server to be used for SMTP authentication for the outbound IP address.	Server IP address or host name and (optional) port number, in the format: server:portnumber
delete	Deletes the outbound IP address.	<b>true</b> : Deletes the outbound IP address.
bcc	Sends a copy of every delivered message to this Email Security archive collection address.	Email address.
account	Moves the outbound IP address from the existing account to the specified account.	UID of the account to move the outbound IP address to.
spoolerduration	Maximum amount of time in hours that mail will be stored (spooled) on the system before it is bounced back to the sender in the event of mail server failure.	Integer from 1 through 320.
retaindelivered	Attribute for keeping legitimate mail.	true or false
authrequired	Specifies that authentication is required.	<b>true</b> : Requires authentication. <b>false</b> : Authentication is optional.
sessiontls	Encryption setting between the outbound IP and the product.	<b>none</b> : Encryption never offered during the session.



Attribute	Description	Valid Options
		<p>available: If an encrypted session cannot be established, the message is sent in the clear.</p> <p><b>required:</b> If an encrypted session can not be established, the connection is closed.</p>
mphuser	Maximum messages per hour allowed for a known sender.	Non-negative integer.
mphother	Maximum messages per hour allowed for all unknown senders combined.	Non-negative integer.
mphuserresponse	Response code and message sent when the limit is exceeded for known senders.	3 digit code, 1 space, message with maximum length of 500.
mphotherresponse	Response code and message sent when the limit is exceeded for all unknown senders combined.	3 digit code, 1 space, message with maximum length of 500.
dsn	IP address-level command that enables or disables the sending of a Delivery Status Notification (DSN) to the sender of a quarantined outbound messages.	<p><b>true:</b> Allows notification of outbound filtered messages.</p> <p><b>false:</b> Disallows notification of outbound filtered messages.</p>
dsnlimit	IP address-level command that sets the number of times per hour a Delivery Status Notification (DSN) message can be sent to the sender alerting them that an outbound message has been quarantined.	Integer 1 through 99999 or "unlimited".
dsnunrestricted	Notification of quarantined message is sent to sender from an unknown outbound IP address.	true or false

Attribute	Description	Valid Options
rcptlimit	Maximum number of message recipients allowed per sender per 6 minute period.	Integer 1 through 99999, or "unlimited".
gateway	Default route for all outbound messages.	<b>null</b> or "": use gateway defined by the MX records <b>hostname</b> : All outbound mail is sent to this server.
annotation	Enable/disable and set location of annotation in message.	<b>None</b> : No Annotation. <b>prepend</b> : The annotation will be inserted at the beginning of the message. <b>append</b> : The annotation will be inserted at the end of the message.
routeGateway	The destination mail server when the action is Special Route.	Hostname or IP address.
securemaildelivery	Whether the Special Route destination is the Encryption service. Note that Encryption must be licensed for this attribute to have an effect.	<b>true</b> : The Special Route destination is the Encryption service. <b>false</b> : Special Route traffic is routed to the server defined in routeGateway.
routeTLSPolicy	Level of encryption to use for the Special Route action.	<b>none</b> : Encryption is never attempted during the session. <b>available</b> : TLS (if available) overrides the Encryption service for special routing. <b>required</b> : If an encrypted session can not be established the connection is closed. <b>valid</b> : The certificate must be valid. <b>trusted</b> : The certificate must be trusted.

### annotation

<annotation> : Child element of <outbound>.

Place the annotation text between the start and end annotation tags.

It is recommended that the annotation be wrapped in a CDATA node to preserve newlines.

The annotation can contain simple HTML tags that will be rendered as text when annotating a text email. Note that the HTML tags must be encoded so the system does not parse it as XML. For example, use `&lt;br/&gt;` to represent `<br/>`.

### categories

`<categories>` : Child element of `<outbound>`.

### category

`<category>` : Child element of `<categories>` and `<outbound>`.

Use the `<category>` element to add or update a specific category. To specify the complete and authoritative set of category-based delivery policies, enclose one or more `<category>` elements in a `<categories>` element. Using the `<categories>` element overrides the existing defaults.

Attribute	Description	Valid Options
name	Message type. (Required)	Virus, adult, phish, bot, spam, pdf, macro, credit, ssn, health, finance, profanity, unscanned.
action	The delivery option for mail in the category. If no action is specified, the category is removed. (Required)	<p><b>allow</b>: Allows the mail to pass to the user's mailbox.</p> <p><b>bcc</b>: Sends messages via bcc to one or more recipients. Recipients are specified using the markup attribute.</p> <p><b>markup</b>: Allows the mail to pass to the user's mailbox with prepended text in the subject line. The markup prefix is specified using the markup attribute.</p> <p><b>route</b>: Sends the mail via the Special Route defined in the Outbound element.</p> <p><b>strip</b>: Strips (permanently deletes) the attachment and delivers the message with an annotation specifying how many attachments were stripped.</p> <p><b>quarantine</b>: Sends the mail to the quarantine.</p> <p><b>block</b>: Deletes the mail.</p>
markup	Text string prepended to the subject line of marked up mail. (Required if action is markup.)	Up to 50 alphanumeric characters.

**contentfilters**

<contentfilters> : Child element of <outbound>.

**contentfilter**

<contentfilter> : Child element of <contentfilters> and <outbound>.

Use the <contentfilter> element to add or update a specific content filter. To specify the complete and authoritative set of content filter-based delivery policies, enclose the <contentfilter> elements in a <contentfilters> element.

Attribute	Description	Valid Options
uid	UID of the content filter. (Required)	GUID of a content filter.
action	Action to take on the content filter. If no action is specified, the content filter is removed. (Required)	<p><b>allow</b>: Allows the mail to pass to the user's mailbox.</p> <p><b>bcc</b>: Sends messages via bcc to one or more recipients. Recipients are specified using the markup attribute.</p> <p><b>route</b>: Routes messages according to instructions set up in Special Routing.</p> <p><b>encrypt</b>: Sends messages as encrypted attachments. The accompanying message instructs the recipient to log in to the secure server to decrypt and view the content of the attached message.</p> <p><b>markup</b>: Allows the mail to pass to the user's mailbox with prepended text in the subject line. The markup prefix is specified using the markup attribute.</p> <p><b>quarantine</b>: Sends the mail to the quarantine.</p> <p><b>block</b>: Deletes the mail.</p>
markup	Text string to prepend the subject line of marked up text. (Required if action is markup.)	For route and encrypt actions, use option <b>dlpOverride</b> to have this content filter's actions override the Compliance filter's actions. For other actions, use text string.

**enemies**

<enemies> : Child element of <outbound>.

**enemy**

<enemy> : Child element of <enemies> and <outbound>.

Use the <enemy> element to add or update an individual non-trusted mail source to automatically quarantine. To specify the complete and authoritative list of enemies, enclose the <enemy> elements in an <enemies> element. Using the <enemies> element overrides the existing enemies list.

Attribute	Description	Valid Options
name	Name of email address to quarantine.	Email address, domain, IP address, country code.
delete	Optional attribute to delete a name from the list.	<b>true</b> : Deletes the name from the list. <b>false</b> : Does not delete the name from the list.

### exemptrecipients

<exemptrecipients> : Child element of <outbound>. Messages to these recipients are not filtered.

### exemptrecipient

<exemptrecipient> : Child element of <exemptrecipients> and <outbound>.

Use the <exemptrecipient> element to add or update an individual recipient. To specify the complete and authoritative recipient whitelist, enclose the <exemptrecipient> element in an <exemptrecipients> element. Using the <exemptrecipients> element overrides the existing recipient whitelist.

Attribute	Description	Valid Options
name	Messages sent to this recipient won't be filtered.	Email address, domain, IP address, country code.
delete	Optional attribute to delete a name from the list.	<b>true</b> : Deletes the name from the list. <b>false</b> : Does not delete the name from the list.

### extensions

<extensions> : Child element of <outbound>.

### extension

<extension> : Child element of <extensions> and <outbound>.

Use the <extension> element to add or update a specific extension. To specify the complete and authoritative set of extension-based delivery policies, enclose the <extension> elements in an <extensions> element. Using the <extensions> element overrides the existing defaults.

Attribute	Description	Valid Options
name	File extension. (Required)	<b>Note:</b> The "." should not be specified.
action	Action to take on file extensions of attached messages. If no action is specified, the extension is removed. (Required)	<b>allow:</b> Allows the mail to pass to the user's mailbox. <b>markup:</b> Allows the mail to pass to the user's mailbox with prepended text in the subject line. The markup prefix is specified using the markup attribute. <b>quarantine:</b> Sends the mail to the quarantine. <b>block:</b> Deletes the mail.
markup	Text string to prepend the subject line of marked up text. (Required if action is markup.)	

## friends

<friends> : Child element of <outbound>.

## friend

<friend> : Child element of <friends> and <outbound>.

Use the <friend> element to add or update an individual trusted mail source. To specify the complete and authoritative list of friends, enclose the <friend> element in a <friends> element. Using the <friends> element overrides the existing friends list.

Attribute	Description	Valid Options
name	Messages from this sender won't be filtered.	Email address, domain, IP address, country code.
delete	Optional attribute to delete a name from the list.	<b>true:</b> Deletes the name from the list. <b>false:</b> Does not delete the name from the list.

## gateways

<gateways> : Child element of <outbound>.

## gateway

<gateway> : Child element of <gateways> and <outbound>.

Use the <gateway> element to add or update a routing exception. To specify the complete and authoritative set of exception routes, enclose the <gateway> elements in an <gateways> element.

Attribute	Description	Valid Options
domain	Mail for this domain does not follow the default route.	Valid domain name
value	Destination server.	Server host name

### properties

<properties> : Child element of <outbound>.

### property

<property> : Child element of <properties> and <outbound>.

Use the <property> element to add or update authentication specifications. To specify the complete and authoritative set of language-based delivery policies, enclose the <property> elements in a <properties> element. Using the <properties> element overrides the existing defaults.

Attribute	Description	Valid Options
captchaLimit	The number of failed login attempts that generates a captcha challenge.	Positive integer.
passwordExpiration	The number of days between required user password resets.	Positive integer.
passwordLength	The number of characters required for a valid password.	Positive integer.
passwordLower	Whether the password requires a lowercase character.	<b>true:</b> The password must contain at least one lowercase character. <b>false:</b> The password does not require a lowercase character.

Attribute	Description	Valid Options
passwordNumber	Whether the password requires a number.	<b>true:</b> The password must contain at least one number. <b>false:</b> The password does not require a number.
passwordSpace	Whether the password requires a space.	<b>true:</b> The password must contain at least one space. <b>false:</b> The password does not require a space.
passwordSpecial	Whether the password requires a special (non-alphanumeric) character.	<b>true:</b> The password must contain at least one special character. <b>false:</b> The password does not require a special character.
passwordUpper	Whether the password requires a uppercase character.	<b>true:</b> The password must contain at least one uppercase character. <b>false:</b> The password does not require a uppercase character.
removeOutboundReceivedHeaders	Whether to remove the internal 'Received' headers.	<b>true:</b> The header is removed. <b>false:</b> The header is not removed.
sessionTimeout	The number of minutes before the dashboard returns to the login screen.	Positive integer.
encryptTlsFailover	Whether to use encryption on messages if TLS encryption is unavailable	<b>E:</b> Attach Encrypted <b>R:</b> Special Routing

### tlsdomains

<tlsdomains> : Child element of <outbound>.

Use the <tlsdomains> element to set the default encryption policy for all outbound traffic between the product and the Internet.



Attribute	Description	Valid Options
policy	Default encryption policy for the outbound IP.	<b>none</b> : Encryption never attempted during the session. <b>available</b> : If an encrypted session cannot be established, the message is sent in the clear. <b>required</b> : If an encrypted session can not be established then the connection is closed <b>valid</b> : The certificate must be valid. <b>trusted</b> : The certificate must be trusted.

<tlsdomain> : Child element of <tlsdomains>.

Use the <tlsdomain> element to override the default encryption policy of a specific outbound IP.

Attribute	Description	Valid Options
name	Name of the domain.	Fully qualified domain name.
policy	Default encryption policy for the outbound IP.	<b>none</b> : Encryption never attempted during the session. <b>available</b> : If an encrypted session cannot be established, the message is sent in the clear. <b>required</b> : If an encrypted session can not be established then the connection is closed <b>valid</b> : The certificate must be valid. <b>trusted</b> : The certificate must be trusted.
hostname	Certificate hostname to validate. (Optional)	domain name, IP address
signature	Certificate signature to validate. (Optional)	base64 encoded certificate signature
specialroutingexempt	Whether this domain is exempt from special routing. (Optional)	<b>true</b> : Domain is exempt from special routing. <b>false</b> : Domain is included in special routing.

## Group Settings

When setting up a group, you can specify the settings that apply to all users in the group. Elements and attributes not specified for the group derive their values from domain or outbound IP settings. On update, an element or attribute not specified is not changed. The following sections show group level elements and tables with their attributes. Note that all attributes are optional unless specified as required.

**groups**

<groups> : Child element of <configuration>.

**group**

<group> : Child element of <groups> and <configuration>.

Use the <group> element to add or update an individual group. To specify the complete and authoritative list of groups, enclose the <group> elements in a <groups> element.

Attribute	Description	Valid Options
name	The name of the group. (Required)	
domainname	The domain to which the group belongs. (Required)	Domains in the system.
grouppriority	The level of priority this group has in the list of groups. If a user belongs to more than one group the settings for the group with a higher priority (lower value) takes precedence. (Required)	Integer.
type	The type of settings specified. (Required)	Inbound or Outbound.
uid	ID, read-only, use for update and delete.	UID of the group.
retainblocked	Attribute for handling blocked mail. (Inbound only)	<b>true</b> : Blocked mail is kept in the administrative quarantine. <b>false</b> (default): Blocked mail is deleted.
retaindelivered	Attribute for keeping legitimate mail.	true or false.
gateway	Inbound: Comma separated list of the domain gateways. Outbound: Default route for all outbound messages.	Inbound: Mail server. Outbound: <b>null</b> or "": use gateway defined by the MX records. <b>hostname</b> : All outbound mail is sent to this server.

Attribute	Description	Valid Options
balanced	How mail is distributed when multiple mail gateways are configured. (Inbound only)	<b>false:</b> Mail is sent to the first entered server. If the server is unavailable, mail goes to the second server, and so on. <b>true:</b> Mail is evenly distributed between all configured servers.
odi	The method for handling mailbox aliases when forwarding to the mail gateway. (Inbound only)	<b>true:</b> Preserves the mailbox alias before sending the message to the mail gateway. <b>false:</b> Rewrites the alias with the primary SMTP address.
maxmsgsize	The maximum size of an individual message. Measured in megabytes. Messages of a size greater than the defined maximum are rejected by the mail server.	Integer from 1 through 100.
spoolerduration	Maximum amount of time in hours that mail will be stored (spooled) on the system before it is bounced back to the sender in the event of mail server failure.	Integer from 1 through 320.
clienttls	Encryption setting between the product and the mail gateway. (Inbound only)	<b>none:</b> Encryption never offered during the session. <b>available:</b> If an encrypted session cannot be established, the message is sent in the clear. <b>required:</b> If an encrypted session can not be established then the connection is closed. <b>valid:</b> The certificate must be valid. <b>trusted:</b> The certificate must be trusted.
bcc	Sends a copy of every delivered message to this product archive collection address.	Email address.
timezone	Time zone of the domain or outbound IP address.	See <a href="#">Supported Time Zones</a> for a list of supported time zones.

Attribute	Description	Valid Options
dsn	IP address-level command that enables or disables the sending of a Delivery Status Notification (DSN) to the sender of a quarantined outbound messages. (Outbound only)	<b>true</b> : Allows notification of outbound filtered messages. <b>false</b> : Disallows notification of outbound filtered messages.
dsnlimit	IP address-level command that sets the number of times per hour a Delivery Status Notification (DSN) message can be sent to the sender alerting them that an outbound message has been quarantined. (Outbound only)	Integer 1 through 99999 or unlimited.
mphuser	Maximum messages per hour allowed for a known sender. (Outbound only)	Non-negative integer.
mphother	Maximum messages per hour allowed for all unknown senders combined. (Outbound only)	Non-negative integer.
mphuserresponse	Response code and message sent when the limit is exceeded for known senders. (Outbound only)	3 digit code, 1 space, message with maximum length of 500.
mphotherresponse	Response code and message sent when the limit is exceeded for all unknown senders combined. (Outbound only)	3 digit code, 1 space, message with maximum length of 500.
annotation	Enable/disable and set location of annotation in message. (Outbound only)	<b>None</b> : No annotation. <b>prepend</b> : The annotation will be inserted at the beginning of the message. <b>append</b> : The annotation will be inserted at the end of the message.

Attribute	Description	Valid Options
sessiontls	Encryption setting between the outbound IP and the product. (Outbound only)	<p><b>none:</b> Encryption never offered during the session.</p> <p><b>available:</b> If an encrypted session cannot be established, the message is sent in the clear.</p> <p><b>required:</b> If an encrypted session can not be established then the connection is closed.</p>

### annotation

<annotation> : Child element of <group> (outbound only).

Place the annotation text between the start and end annotation tags.

It is recommended that the annotation be wrapped in a CDATA node to preserve newlines.

The annotation can contain simple HTML tags that will be rendered as text when annotating a text email. Note that the HTML tags must be encoded so the system does not parse it as XML. For example, use &lt;br/&gt; to represent <br/>.

### categories

<categories> : Child element of <group>.

### category

<category> : Child element of <categories> and <group>.

Use the <category> element to add or update a specific category. To specify the complete and authoritative set of category-based delivery policies, enclose one or more <category> elements in a <categories> element. Using the <categories> element overrides the existing defaults.

Attribute	Description	Valid Options
name	Message type. (Required)	Virus, adult, phish, bot, spam, pdf, macro, junk, credit, ssn, health, finance, profanity.

Attribute	Description	Valid Options
action	The delivery option for mail in the category. If no action is specified, the category is removed. (Required)	<b>allow</b> : Allows the mail to pass to the user's mailbox. <b>markup</b> : Allows the mail to pass to the user's mailbox with prepended text in the subject line. The markup prefix is specified using the markup attribute. <b>strip</b> : Strips (permanently deletes) the attachment and delivers the message with an annotation specifying how many attachments were stripped. <b>quarantine</b> : Sends the mail to the quarantine. <b>block</b> : Deletes the mail.
markup	Text string prepended to the subject line of marked up mail. (Required if action is markup.)	Up to 50 alphanumeric characters.

## console

<console> : Child element of <group> (inbound only).

Attribute	Description	Valid Options
enabled	If false, the console will not be available to users in this group.	true or false
quarantine	If false, users will not have access to their personal quarantine.	true or false
outbound	If false, users will not have access to their outbound quarantine.	true or false
settings	If false, users will not be able to change settings (such as digest settings, time zone, etc.).	true or false
policies	If false, users will not be able to change disposition policies for messages based on category.	true or false

Attribute	Description	Valid Options
foreign	If false, users will not be able to change disposition policies based on languages (i.e., character sets).	true or false
attachments	If false, users will not be able to change dispositions based on attachment file extensions.	true or false
sender	If false, users will not be able to change dispositions based on senders such as friends/enemies list.	true or false
release	If false, users cannot release inbound mail from the quarantine.	true or false
outboundRelease	If false, users cannot release outbound mail from the quarantine.	true or false
dlprelease	If false, users cannot release DLP messages from the quarantine.	true or false
messagedelete	If false, users cannot delete messages from the quarantine.	true or false

### contentfilters

<contentfilters> : Child element of <group>.

### contentfilter

<contentfilter> : Child element of <contentfilters> and <group>.

Use the <contentfilter> element to add or update a specific content filter. To specify the complete and authoritative set of content filter-based delivery policies, enclose the <contentfilter> elements in a <contentfilters> element.

Attribute	Description	Valid Options
uid	UID of the content filter. (Required)	GUID of a content filter.

Attribute	Description	Valid Options
action	Action to take on the content filter. If no action is specified, the content filter is removed. (Required)	<b>allow</b> : Allows the mail to pass to the user's mailbox. <b>markup</b> : Allows the mail to pass to the user's mailbox with prepended text in the subject line. The markup prefix is specified using the markup attribute. <b>quarantine</b> : Sends the mail to the quarantine. <b>block</b> : Deletes the mail.
markup	Text string to prepend the subject line of marked up text. (Required if action is markup.)	Text string.

## digest

<digest> : Child element of <group> (inbound only).

Attribute	Description	Valid Options
detail	Controls the (minimum) level of detail on the digest. (At least one attribute required.)	<b>summary</b> : Summary only. <b>green</b> : Displays only mail from the green zone (junk). <b>yellow</b> : Displays mail from the yellow zone (foreign, attachments) plus mail from the green zone. <b>red</b> : Displays all mail in the quarantine.
format	Format of the daily digest. (At least one attribute required.)	Text, html, or multipart.
frequency	The delivery frequency of the digest. (At least one attribute required.)	<b>never</b> : The digest is not sent. <b>daily</b> : The digest is sent every day. <b>weekly</b> : The digest is sent once a week.
language	The digest language.	<b>Inherit</b> : The digest is in the language specified for the domain. <b>English</b> : The digest is in English.



Attribute	Description	Valid Options
order	The order the messages in the digest are sorted. (At least one attribute required.)	<b>Date-</b> : Sorts from newest to oldest. <b>Date+</b> : Sorts from oldest to newest. <b>Size-</b> : Sorts from largest to smallest. <b>Size+</b> : Sorts from smallest to largest. <b>Mailbox</b> : Sorts on the "SMTP Mail From" field. <b>Sender</b> : Sorts on the "From" field in the Mime Header. <b>Subject</b> : Sorts by subject.

### enemies

<enemies> : Child element of <group>.

### enemy

<enemy> : Child element of <enemies> and <group>.

Use the <enemy> element to add or update an individual non-trusted mail source to automatically quarantine. To specify the complete and authoritative list of enemies, enclose the <enemy> elements in an <enemies> element. Using the <enemies> element overrides the existing enemies list.

Attribute	Description	Valid Options
name	Name of email address to quarantine.	Email address, domain, IP address, country code.
delete	Optional attribute to delete a name from the list.	<b>true</b> : Deletes the name from the list. <b>false</b> : Does not delete the name from the list.

### exemptrecipients

<exemptrecipients> : Child element of <group> (outbound only). Messages to these recipients are not filtered.

### exemptrecipient

<exemptrecipient> : Child element of <exemptrecipients> and <group>.

Use the <exemptrecipient> element to add or update an individual recipient. To specify the complete and authoritative recipient whitelist, enclose the <exemptrecipient> element in an <exemptrecipients> element. Using the <exemptrecipients> element overrides the existing recipient whitelist.

Attribute	Description	Valid Options
name	Messages sent to this recipient won't be filtered.	Email address, domain, IP address, country code.
delete	Optional attribute to delete a name from the list.	<b>true</b> : Deletes the name from the list. <b>false</b> : Does not delete the name from the list.

### extensions

<extensions> : Child element of <group>.

### extension

<extension> : Child element of <extensions> and <group>.

Use the <extension> element to add or update a specific extension. To specify the complete and authoritative set of extension-based delivery policies, enclose the <extension> elements in an <extensions> element. Using the <extensions> element overrides the existing defaults.

Attribute	Description	Valid Options
name	File extension. (Required)	<b>Note</b> : The "." should not be specified.
action	Action to take on file extensions of attached messages. If no action is specified, the extension is removed. (Required)	<b>allow</b> : Allows the mail to pass to the user's mailbox. <b>markup</b> : Allows the mail to pass to the user's mailbox with prepended text in the subject line. The markup prefix is specified using the markup attribute. <b>quarantine</b> : Sends the mail to the quarantine. <b>block</b> : Deletes the mail.
markup	Text string to prepend the subject line of marked up text. (Required if action is markup.)	

### friends

<friends> : Child element of <group>.

### friend

<friend> : Child element of <friends> and <group>.

Use the <friend> element to add or update an individual trusted mail source. To specify the complete and authoritative list of friends, enclose the <friend> element in a <friends> element. Using the <friends> element overrides the existing friends list.

Attribute	Description	Valid Options
name	Messages from this sender won't be filtered.	Email address, domain, IP address, country code.
delete	Optional attribute to delete a name from the list.	<b>true:</b> Deletes the name from the list. <b>false:</b> Does not delete the name from the list.

## languages

<languages> : Child element of <group> (inbound only).

### language

<language> : Child element of <languages> and <group>.

Use the <language> element to add or update a specific language. To specify the complete and authoritative set of language-based delivery policies, enclose the <language> elements in a <languages> element. Using the <languages> element overrides the existing defaults.

Attribute	Description	Valid Options
name	Character set name. (Required)	See <a href="#">Language Codes</a> for the list of supported languages.
action	Action to take on messages in selected language. If no action is specified, the language is removed. (Required)	<b>allow:</b> Allows the mail to pass to the user's mailbox. <b>markup:</b> Allows the mail to pass to the user's mailbox with prepended text in the subject line. The markup prefix is specified using the markup attribute. <b>quarantine:</b> Sends the mail to the quarantine. <b>block:</b> Deletes the mail.
markup	Text string prepended to the subject line of marked up mail. (Required if action is markup.)	Up to 50 alphanumeric characters.

**properties**

<properties> : Child element of <group>.

**property**

<property> : Child element of <properties> and <group>.

Use the <property> element to add or update authentication specifications. To specify the complete and authoritative set of language-based delivery policies, enclose the <property> elements in a <properties> element. Using the <properties> element overrides the existing defaults.

Attribute	Description	Valid Options
captchaLimit	The number of failed login attempts that generates a captcha challenge.	Positive integer.
includeOutbound	Whether outbound messages are included in the spam digest.	<b>true</b> : The spam digest includes outbound messages. <b>false</b> : The spam digest does not include outbound messages.
passwordExpiration	The number of days between required user password resets.	Positive integer.
passwordLength	The number of characters required for a valid password.	Positive integer.
passwordLower	Whether the password requires a lowercase character.	<b>true</b> : The password must contain at least one lowercase character. <b>false</b> : The password does not require a lowercase character.
passwordNumber	Whether the password requires a number.	<b>true</b> : The password must contain at least one number. <b>false</b> : The password does not require a number.
passwordSpace	Whether the password requires a space.	<b>true</b> : The password must contain at least one space. <b>false</b> : The password does not require a space.
passwordSpecial	Whether the password requires a special (non-alphanumeric) character.	<b>true</b> : The password must contain at least one special character. <b>false</b> : The password does not require a special character.

Attribute	Description	Valid Options
passwordUpper	Whether the password requires a uppercase character.	<b>true</b> : The password must contain at least one uppercase character. <b>false</b> : The password does not require a uppercase character.
sessionTimeout	The number of minutes before the dashboard returns to the login screen.	Positive integer.

## tlsdomains

<tlsdomains> : Child element of <group> (outbound only).

Use the <tlsdomains> element to set the default encryption policy for all outbound traffic between the product and the Internet for this group.

Attribute	Description	Valid Options
policy	Default encryption policy for the group.	<b>none</b> : Encryption never attempted during the session. <b>available</b> : If an encrypted session cannot be established, the message is sent in the clear. <b>required</b> : If an encrypted session can not be established then the connection is closed <b>valid</b> : The certificate must be valid. <b>trusted</b> : The certificate must be trusted.

## Brand Settings

When creating a domain, elements and attributes not specified derive their values from brand level defaults. If no brand level defaults exist, system defaults are used.

When creating an Outbound IP, elements and attributes not specified derive their values from system defaults.

The <outbound-defaults> settings are used to filter outbound traffic from senders not located in any of the configured outbound IP ranges.

On brand element updates, an attribute not specified is not changed. Note that brand level elements are accessible only to System Administrators.

### domain-defaults

<domain-defaults> : The child element of <configuration>.

There can be only one <domain-defaults> element per brand. If there are multiple entries, the last entry is used.

The attributes for this element are the same as for the <domain> element. See [domain](#) for details.

**outbound-defaults**

<outbound-defaults> : The child element of <configuration>.

There can be only one <outbound-defaults> element per brand. If there are multiple entries, the last entry is used.

The attributes for this element are the same as the attributes for Outbound IP settings for the <outbound> element. See [outbound](#) for details.

**Mailbox Settings**

The following sections show mailbox-level elements and tables with their attributes. Note that all attributes are optional unless specified as required. When attributes are not specified at the mailbox level, the domain settings apply.

**mailboxes**

<mailboxes> : Child element of <domain>.

**mailbox**

<mailbox> : Child element of <mailboxes> and <domain>.

Use the <mailbox> element to add or update a specific mailbox. To specify the complete and authoritative set of mailboxes, enclose the <mailbox> element in a <mailboxes> element.

Attribute	Description	Valid Options
name	The name of the mailbox in the domain. (Required)	
status	Mailbox status.	active: The mailbox is active. This is the default state. unprotected: No messages for this mailbox are filtered. failure: Verifier determined invalid mailbox. Note that the API cannot be used to set the status to failure, this status is read-only. inactive: The mailbox is an alias for another mailbox or mail is not filtered for it.
timezone	Time zone of the mailbox. If the timezone attribute is not specified, the value of the domain timezone will be used.	See <a href="#">Supported Time Zones</a> for a list of supported time zones.
bcc	Blind copy field of email "to" address.	Email address.

Attribute	Description	Valid Options
delete	Deletes the mailbox.	true: Deletes the mailbox.
consoleaccess	Determines whether user has access to the dashboard and receives the digest.	true or false.
annotation	Can be set to 'none' to override the outbound IP setting.	none: Annotation is not added to messages sent by this user.
mph	Sender override on messages per hour outbound rate limiting.	mph -1: unlimited positive integer: rate per 6 min. "" : use outbound IP setting
rcptlimit	Sender override on recipients per message per 6-minute rate limit.	-1: unlimited positive integer: rate per hour "" : use outbound IP setting

## alias

<alias> : Child element of <mailbox>.

Attribute	Description	Valid Options
name	The alias of the mailbox. (Required)	Email address.

## categories

<categories > : Child element of <mailbox>.

## category

<category> : Child element of <categories> and <mailbox>.

Use the <category> element to add or update a specific category. To specify the complete and authoritative set of category-based delivery policies, enclose the <category> elements in a <categories> element. Using the <categories> element overrides the existing defaults.

Attribute	Description	Valid Options
name	Message type. (Required)	Virus, adult, phish, bot, spam, junk, credit, ssn.

Attribute	Description	Valid Options
action	The delivery option for mail in the category. If no action is specified, the category is removed. (Required)	<b>allow</b> : Allows the mail to pass to the user's mailbox. <b>markup</b> : Allows the mail to pass to the user's mailbox with prepended text in the subject line. The markup prefix is specified using the markup attribute. <b>strip</b> : Strips (permanently deletes) the attachment and delivers the message with an annotation specifying how many attachments were stripped. <b>quarantine</b> : Sends the mail to the quarantine. <b>block</b> : Deletes the mail.
markup	Text string prepended to the subject line of marked up mail. (Required if action is markup.)	Up to 50 alphanumeric characters.

## console

<console> : Child element of <mailbox>. Console settings.

An empty string for the value of a console attribute indicates that its value should be inherited from the domain setting.



**Note:** If enabled is false, the other attributes are irrelevant.

Attribute	Description	Valid Options
enabled	If false, the console will not be available to users in this domain.	true or false
quarantine	If false, users will not have access to their personal quarantine.	true or false
outbound	If false, users will not have access to their outbound quarantine.	true or false
settings	If false, users will not be able to change settings (such as digest settings, time zone, etc.).	true or false
policies	If false, users will not be able to change disposition policies for messages based on category.	true or false



Attribute	Description	Valid Options
foreign	If false, users will not be able to change disposition policies based on languages (i.e., character sets).	true or false
attachments	If false, users will not be able to change dispositions based on attachment file extensions.	true or false
senders	If false, users will not be able to change dispositions based on senders such as friends/enemies list.	true or false
release	If false, users cannot release mail from the quarantine.	true or false
dlprelease	If false, users cannot release DLP messages from the quarantine.	true or false
messagedelete	If false, users cannot delete messages from the quarantine.	true or false

## digest

<digest> : Child element of <mailbox>.



**Note:** Use inherit for a parameter when you want it to have the same setting as the domain.

Attribute	Description	Valid Options
detail	Controls the (minimum) level of detail on the digest. (At least one attribute required.)	<b>summary:</b> Summary only. <b>green:</b> Displays only mail from the green zone (junk). <b>yellow:</b> Displays mail from the yellow zone (foreign, attachments) plus mail from the green zone. <b>red:</b> Displays all mail from the quarantine.
format	Format of the daily digest. (At least one attribute required.)	Text or html.

Attribute	Description	Valid Options
frequency	The frequency of the digest. If set to inherit, it uses the domain settings. (At least one attribute required.)	<b>never</b> : Does not send the digest. <b>daily</b> : Sends the digest every day. <b>weekly</b> : Sends the digest once a week.
order	The order the messages in the digest are sorted. If blank, it uses the domain settings. (At least one attribute required.)	<b>Date-</b> : Sorts from newest to oldest. <b>Date+</b> : Sorts from oldest to newest. <b>Size-</b> : Sorts from largest to smallest. <b>Size+</b> : Sorts from smallest to largest. <b>Mailbox</b> : Sorts on the "SMTP Mail From" field. <b>Sender</b> : Sorts on the "From" field in the Mime Header. <b>Subject</b> : Sorts by subject.

## enemies

<enemies> : Child element of <mailbox>.

## enemy

<enemy> : Child element of <enemies> and <mailbox>.

Use the <enemy> element to add or update an individual non-trusted mail source to automatically quarantine. To specify the complete and authoritative list of enemies, enclose the <enemy> elements in an <enemies> element. Using the <enemies> element overrides the existing enemies list.

Attribute	Description	Valid Options
name	Name of email address to quarantine.	Email address, domain, IP address, country code.
delete	Optional attribute to delete a name from the list.	<b>true</b> : Deletes the name from the list. <b>false</b> : Does not delete the name from the list.

## extensions

<extensions> : Child element of <mailbox>.

## extension

<extension> : Child element of <extensions> and <mailbox>.

Use the <extension> element to add or update a specific extension. To specify the complete and authoritative set of extension-based delivery policies, enclose the <extension> elements in an <extensions> element. Using the <extensions> element overrides the existing defaults.

Attribute	Description	Valid Options
name	File extension. (Required)	<b>Note:</b> The "." should not be specified.
action	Action to take on file extensions of attached messages. If no action is specified, the extension is removed. (Required)	<b>allow:</b> Allows the mail to pass to the user's mailbox. <b>markup:</b> Allows the mail to pass to the user's mailbox with prepended text in the subject line. The markup prefix is specified using the markup attribute. <b>quarantine:</b> Sends the mail to the quarantine. <b>block:</b> Deletes the mail.
markup	Text string to prepend the subject line of marked up text. (Required if action is markup.)	

## friends

<friends> : Child element of <mailbox>.

## friend

<friend> : Child element of <friends> and <mailbox>.

Use the <friend> element to add or update an individual trusted mail source. To specify the complete and authoritative list of friends, enclose the <friend> elements in a <friends> element. Using the <friends> element overrides the existing friends list.

Attribute	Description	Valid Options
name	Messages from this sender won't be filtered.	Email address, domain, IP address, country code.
delete	Optional attribute to delete a name from the list.	<b>true:</b> Deletes the name from the list. <b>false:</b> Does not delete the name from the list.

## groups

<groups> : Child element of <mailbox>.

## group

<group> : Child element of <groups> and <mailbox>.

Use the <group> element to specify the groups in which the mailbox is a member.

Attribute	Description	Valid Options
type	The type of group discovery.	Manual or Auto (read only, uses LDAP to populate the group).

### languages

<languages> : Child element of <mailbox>.

### language

<language> : Child element of <languages> and <mailbox>.

Use the <language> element to add or update a specific language. To specify the complete and authoritative set of language-based delivery policies, enclose the <language> elements in a <languages> element. Using the <languages> element overrides the existing defaults.

Attribute	Description	Valid Options
name	Character set name. (Required)	See <a href="#">Language Codes</a> for the list of supported languages.
action	Action to take on messages in selected language. If no action is specified, the language is removed.	<b>allow</b> : Allows the mail to pass to the user's mailbox. <b>markup</b> : Allows the mail to pass to the user's mailbox with prepended text in the subject line. The markup prefix is specified using the markup attribute. <b>quarantine</b> : Sends the mail to the quarantine. <b>block</b> : Deletes the mail.
markup	Text string prepended to the subject line of marked up mail. (Required if action is markup.)	Up to 50 alphanumeric characters.

### properties

<properties> : Child element of <mailbox>.

### property

<property> : Child element of <properties> and <mailbox>.

Use the <property> element to add or update authentication specifications. To specify the complete and authoritative set of language-based delivery policies, enclose the <property> elements in a <properties> element. Using the <properties> element overrides the existing defaults.

Attribute	Description	Valid Options
captchaLimit	The number of failed login attempts that generates a captcha challenge.	Positive integer.
passwordExpiration	The number of days between required user password resets.	Positive integer.
passwordLength	The number of characters required for a valid password.	Positive integer.
passwordLower	Whether the password requires a lowercase character.	<b>true:</b> The password must contain at least one lowercase character. <b>false:</b> The password does not require a lowercase character.
passwordNumber	Whether the password requires a number.	<b>true:</b> The password must contain at least one number. <b>false:</b> The password does not require a number.
passwordSpace	Whether the password requires a space.	<b>true:</b> The password must contain at least one space. <b>false:</b> The password does not require a space.
passwordSpecial	Whether the password requires a special (non-alphanumeric) character.	<b>true:</b> The password must contain at least one special character. <b>false:</b> The password does not require a special character.
passwordUpper	Whether the password requires an uppercase character.	<b>true:</b> The password must contain at least one uppercase character. <b>false:</b> The password does not require an uppercase character.
sessionTimeout	The number of minutes before the dashboard returns to the login screen.	Positive integer.

## Language Codes

The table below shows the languages supported in the Email Security XML API. Lower case codes are used for actual languages, uppercase codes are used for groups of languages.

Code	Language	Code	Language
ar	Arabic	ko	Korean
BS	Baltic	NO	Nordic
CC	Celtic	tr	Turkish
CY	Cyrillic	th	Thai
zy	Chinese	CE	Central European
el	Greek	EE	Eastern European
he	Hebrew	SE	Southern European
ja	Japanese		



**Note:** Country codes are case-sensitive.

## CHAPTER 6      Sample XML Code

The following code samples show examples of the Email Security API.

### Download Account List

To get a list of UIDs:

```
curl "http://$DASHBOARD/api/account/list?token=$TOKEN"
```

To get a subset on the server:

```
curl "http://$DASHBOARD/api/account/list?token=$TOKEN&name=ad"
```

This returns a list of accounts starting with the string "ad".



**Note:** The text string between the quotation marks "%20" signifies a space in the command. For example "name=Any%20Company". To ensure that the URL is valid, encode spaces as "%20".

### Download Domain List

To get a list of all the domains associated with an account <UID>:

```
curl "http://$DASHBOARD/api/config/download?token=$TOKEN&account=<UID>"
```

To further refine the search, use the domain=str tag. The following example downloads all domains in the specified account that begin with ad:

```
curl "http://$DASHBOARD/api/config/download?token=$TOKEN&account=<UID>&domain=ad"
```

### Viewing the Account Configuration

Issue the following command to see the account configuration:

```
curl "http://$DASHBOARD/api/account/list?token=$TOKEN&name=$ACCOUNT"
```

Where \$ACCOUNT is the UID of the account.

The following shows sample output from the above command:

```
<result>
<account name="My Company" uid="4719F67E-8854-F6EA-0997-40976869F3A6"
created="2011-04-28T21:17:28.687" modified="2011-04-28T21:17:28.687"
contact="Joe Schmo" phone="707 555 4100" country="US"
timezone="America/Los_Angeles" cluster="example.acme.net"/>
</result>
```

## Adding a Domain

The following is an example of adding a domain.

```
<configuration version="2.2" timestamp="2008-01-21T10:02:51.349">
  <domain name="example.com" account="C653622B-22A1-21BB-CD7F-CAFDFE246F47"
  gateway="mailer.example.com" discovery="disabled" unrecognized="bounce" timezone="america/Los_
  Angeles" authserver="smtp.foo.com">
    <digest detail="summary" format="text" frequency="weekly" order="sender"/>
    <friends>
      <friend name="john@example.com"/>
    </friends>
    <enemies>
      <enemy name="enemy1@enemies.com"/>
      <enemy name="enemy2@enemies.com"/>
    </enemies>
    <categories>
      <category name="virus" action="quarantine"/>
      <category name="adult" action="quarantine"/>
      <category name="phish" action="quarantine"/>
      <category name="spam" action="quarantine"/>
      <category name="junk" action="quarantine"/>
    </categories>
    <languages>
      <language name="ar" action="block"/>
      <language name="BS" action="block"/>
      <language name="CC" action="block"/>
      <language name="CY" action="block"/>
      <language name="zy" action="block"/>
      <language name="el" action="quarantine"/>
      <language name="he" action="quarantine"/>
      <language name="ja" action="quarantine"/>
      <language name="ko" action="quarantine"/>
      <language name="NO" action="quarantine"/>
      <language name="tr" action="allow"/>
      <language name="th" action="allow"/>
      <language name="CE" action="allow"/>
      <language name="EE" action="allow"/>
      <language name="SE" action="allow"/>
    </languages>
    <properties>
      <property key="captchaLimit">11</property>
      <property key="passwordExpiration">31</property>
      <property key="passwordLength">8</property>
      <property key="passwordLower">true</property>
      <property key="passwordNumber">false</property>
      <property key="passwordSpace">false</property>
      <property key="passwordSpecial">false</property>
      <property key="passwordUpper">false</property>
      <property key="sessionTimeout">31</property>
    </properties>
    <extensions>
      <extension name="asd" action="block"/>
      <extension name="bat" action="block"/>
      <extension name="cab" action="block"/>
      <extension name="chm" action="block"/>
      <extension name="com" action="block"/>
      <extension name="cpl" action="block"/>
    </extensions>
  </domain>
</configuration>
```



```

    <extension name="dat" action="block"/>
    <extension name="dll" action="block"/>
    <extension name="eml" action="quarantine"/>
    <extension name="exe" action="quarantine"/>
    <extension name="hlp" action="quarantine"/>
    <extension name="hta" action="quarantine"/>
    <extension name="inf" action="quarantine"/>
    <extension name="lnk" action="quarantine"/>
    <extension name="msi" action="quarantine"/>
    <extension name="msp" action="quarantine"/>
    <extension name="nws" action="markup" markup="null"/>
    <extension name="ocx" action="markup" markup="ocx"/>
    <extension name="pif" action="markup" markup="pif"/>
    <extension name="reg" action="markup" markup="reg"/>
    <extension name="scr" action="markup" markup="scr"/>
    <extension name="sct" action="markup" markup="sct"/>
    <extension name="shb" action="markup" markup="shb"/>
    <extension name="shs" action="markup" markup="shs"/>
  </extensions>
</domain>
</configuration>

```

## Deleting a Domain

The following is an example of deleting the domain example.com.

```

<domain name="example.com" account="C653622B-22A1-21BB-CD7F-CAFDFE246F47" delete="true"/>
</domain>

```

## Moving Domains between Accounts

The following example moves the domain example.com to the account specified in the UID:

```

<domain name="example.com" account="C653622B-22A1-21BB-CD7F-CAFDFE246F47">
  ...
</domain>

```

## Setting the User Dashboard Authentication Method

You can specify a dashboard authentication method for a domain using the standard configuration API. The product supports:

- **Internal:** ID and password are stored on the GoSecure Email Security server.
- **SMTP AUTH:** Uses the SMTP AUTH command for authenticating the user. ID and password are stored on the mail server.
- **LDAP:** Uses Lightweight Directory Access Protocol for authenticating the user. The ID and password are stored on the directory server.

If the authentication method is not specified, the authenticator for the domain will not be modified. To reset the authentication method for the domain, specify an empty string.

### SMTP AUTH

The following command is an example of how to specify SMTP authentication for the domain example.com.

```
<domain name="example.com" authserver="server:portnumber"
"
</domain>
```

Where server:portnumber is the mail server IP address or host name and (optional) port number.

## LDAP

The following command is an example of how to specify LDAP authentication for the domain example.com.

```
<domain name="example.com" authenticator="xxxxxx">
"
</domain>
```

Where xxxxxx is the UID of an LDAP verifier.

## Assigning a Verifier to a Domain

Issue the following command to add an existing verifier to a domain using the standard configuration API.

```
<domain name="example.com" verifier="xxxxxx?">
"
</domain>
```

Where xxxxxx is the UID of the verifier.

If the verifier attribute is not specified, the verifier for the domain will not be modified. To reset the verifier for the domain, specify an empty string.

## Setting the Encryption Policy

The following example forces encryption to be used for all connections from the product to the mail gateway.

```
<domain name="example.com" mbcleanup="3" timezone="" gateway="mail.example.com" discovery="
disabled" unrecognized="discard" odi="true" out boundaccess="false" clienttls="required">
</domain>
```

## Creating User Mailboxes

The following example shows how to create user mailboxes for the domain example.com, add addresses to the friends and enemies list of the aaron mailbox, and add an alias to the adserl mailbox. The adrian mailbox has no Personal Dashboard access.

```
<domain name="example.com">
  <mailbox name="aaron">
    <friend name="temp@acme.com"/>
    <enemy name="TE"/>
  </mailbox>
  <mailbox name="adrian" consoleaccess="false">
  </mailbox>
  <mailbox name="adserl">
    <alias name="adserl@example.net"/>
  </mailbox>
</domain>
```

## Deleting User Mailboxes

The following is an example of deleting a user mailbox.

```
<domain name="example.com" >
  <mailbox name="john" delete="true">
</mailbox>
</domain>
```

## Exempting Recipients from Outbound Rate Limits

The following example shows how to replace the existing exempt recipient list with a new one.

```
<domain name="1.2.3.4/32">
  <exemptrecipients>
    <exemptrecipient name="user@yahoo.com"/>
    <exemptrecipient name="domain.com" delete="true"/>
  </exemptrecipients>
</domain>
```

The following example shows how to add an address to the exempt recipient list.

```
<domain name="1.2.3.4/32">
  <exemptrecipient name="user@yahoo.com"/>
</domain>
```

## Modifying Friends and Enemies Lists

The following example shows how to add an individual user to the friends and enemies lists after the mailbox has been created.

```
<friend name="friend@friends.com"/>
<enemy name="enemy@enemies.com"/>
```

The following example shows how to delete an individual user from the friends and enemies lists after the mailbox has been created.

```
<friend name="friend@friends.com" delete="true"/>
<enemy name="enemy@enemies.com" delete="true"/>
```

The following example shows how to create multiple entries into each the friends and enemies lists. All other entries in the list will be deleted.



**Warning!** Adding and deleting multiple entries at one time replaces the existing list. It does not append or subtract from the existing list. Use these commands with care.

```
<friends>
  <friend name="friend1@friends.com"/>
  <friend name="friend2@friends.com"/>
</friends>
<enemies>
  <enemy name="enemy1@enemies.com"/>
  <enemy name="enemy2@enemies.com"/>
</enemies>
```

## Authentication Settings

The following example specifies authentication settings for the domain example.com:

```
<domain name="example.com">
  <properties>
    <property key="captchaLimit">11</property>
    <property key="passwordExpiration">31</property>
    <property key="passwordLength">8</property>
    <property key="passwordLower">true</property>
    <property key="passwordNumber">false</property>
    <property key="passwordSpace">false</property>
    <property key="passwordSpecial">false</property>
    <property key="passwordUpper">false</property>
    <property key="sessionTimeout">31</property>
  </properties>
</domain>
```

The following example changes the password length setting for the domain example.com:

```
<domain name="example.com">
  <property key="passwordLength">8</property>
</domain>
```

The following example resets all authentication settings for the domain example.com to the brand defaults:

```
<domain name="example.com">
  <properties/>
</domain>
```

The following example resets all authentication settings for the mailbox to the domain defaults:

```
<mailbox name="john">
  <properties/>
</mailbox>
```

## Category Filter Settings

Delivery policy by category can be specified using the category element. A single category policy can be added, changed, or removed by specifying the category element under the domain or mailbox element. For example:

```
<domain name="example.com">
  <category name="virus" action="markup" markup="VIRUS:"/>
</domain>
```

This sample code will only change the virus delivery for the domain. Unsupported actions will be ignored. If no action is specified, the corresponding delivery policy is removed (and therefore inherited from the domain settings in the case of a mailbox).

To specify the complete and authoritative set of category-based delivery policies, enclose the category elements in a categories element. For example:

```
<domain name="example.com">
  <categories>
    <category name="virus" action="markup" markup="VIRUS:"/>
    <category name="adult" action="markup" markup="ADLT:"/>
    <category name="phish" action="quarantine"/>
  </categories>
</domain>
```

```

    <category name="spam" action="quarantine"/>
  </categories>
</domain>

```

In this case, the complete set of policies is assigned to the domain regardless of any existing policies for the domain. Categories not specified are removed and the system default is used.

## Content Filter Settings

The following example adds a content filter for the domain example.com that quarantines the filtered mail:

```

<domain name="example.com">
  <contentfilter uid="86B88D3C-F29B-6F59-6B0E-6C26603FC18B" action="quarantine"/>
</domain>

```

The following example removes a content filter for the domain example.com:

```

<domain name="example.com">
  <contentfilter uid="86B88D3C-F29B-6F59-6B0E-6C26603FC18B"/>
</domain>

```

The following example removes all content filters for the domain example.com:

```

<domain name="example.com">
  <contentfilters/>
</domain>

```

The following example creates a complete authoritative content filter policy for the domain example.com. No other content filters will be applied to this domain.

```

<domain name="example.com">
  <contentfilters>
    <contentfilter uid="86B88D3C-F29B-6F59-6B0E-6C26603FC18B" action="quarantine"/>
    <contentfilter uid="BFE78762-1788-4DA2-B84F-3C73D3C7EF09" action="quarantine"/>
  </contentfilters>
</domain>

```

The following example updates content filter to mark up a message for the domain example.com.

```

<domain name="example.com">
  <contentfilter uid="52bd2714-a881-4772-acf2-efb82cf53bd7" action="markup"
  markup="CONTENTFILTER:"/>
</domain>

```



**Note:** For details on how to obtain the content filter UID, see [Configuration Download](#).

## Digest Settings

Digest settings can be specified for a domain or mailbox. The settings are controlled by the digest element under the domain or mailbox. For example, for the domain example.com:

```

<domain name="example.com">
  digest detail="red" format="html" frequency="daily" order="Date-"/>
</domain>

```

If an element or attribute is not specified, the corresponding setting will remain unaffected. If the digest element is not specified, none of the digest settings are affected. If a setting is set to inherit (or blank in the case of the order), the setting is set to be inherited (the mailbox settings are derived from the domain settings).

The following is a sample of digest settings for a mailbox:

```
<domain name="example.com">
  <mailbox name="test1">
    <digest detail="red" format="text"/>
  </mailbox>
</domain>
```

## Extension Filter Settings

Extension-based delivery policies are specified using the extension element in a manner similar to the category (and language) policies described above. If no action is specified, the corresponding delivery policy is removed (and therefore inherited from the domain settings in the case of a mailbox). For example:

```
<domain name="example.com">
  <extension name="ext" action="quarantine"/>
</domain>
```

To specify the complete and authoritative set of extension-based delivery policies:

```
<domain name="example.com">
  <extensions>
    <extension name="ext" action="quarantine"/>
    <extension name="jpg" action="markup" markup="null"/>
    <extension name="tib" action="quarantine"/>
    <extension name="zip" action="quarantine"/>
  </extensions>
</domain>
```

This script will replace the complete set of extension-based policies specified for the given domain. Extensions not specified are removed and the system default is used.



**Note:** The period (.) should not be specified.

## Language Filter Settings

Language-based delivery policies are specified using the language element in a manner similar to the category policies described above. For example:

```
<domain name="example.com">
  <language name="he" action="quarantine"/>
</domain>
```

This script will only affect the delivery policy for the Hebrew language. If no action is specified, the corresponding delivery policy is removed (and therefore inherited from the domain settings in the case of a mailbox).

```
<domain name="example.com">
  <languages>
    <language name="BS" action="quarantine"/>
  </languages>
</domain>
```

```

    <language name="CC" action="quarantine"/>
    <language name="CE" action="quarantine"/>
    <language name="CY" action="allow"/>
    <language name="EE" action="block"/>
    <language name="he" action="quarantine"/>
    <language name="tr" action="block"/>
    <language name="zh" action="allow"/>
  </languages>
</domain>

```

This script will replace the complete set of language-based policies specified for the given domain. Languages not specified are removed and the system default is used. Lowercase codes are used for actual languages, uppercase codes are used for groups of languages.

## Groups

The following examples apply to groups.

### Adding a Group

The following is an example of adding a group. It creates a group named SVT Group 2 which overrides the outbound IP's settings for SSN and CCN, and the Domain's gateway and handling of zip file attachments.

```

<configuration version="2.7" timestamp="2013-10-29T17:12:52.493">
  <groups>
    <group name="SVT Group 2" domainname="example.com" grouppriority="1" type="outbound">
      <category name="ssn" action="markup" markup="SSN:"/>
      <category name="credit" action="markup" markup="CC:"/>
    </group>
    <group name="SVT Group 2" domainname="example.com" grouppriority="1" type="inbound"
      gateway="mail.example.com" >
      <extension name="zip" action="markup" markup="ZIP"/>
    </group>
  </groups>
</configuration>

```

### Deleting a Group

This example deletes both the inbound and outbound parts of the group.

```

<group name="SVT Group 2" domainname="example.com" uid="23a6ef94-0589-4e4e-abf6-f8321da7085a"
delete="true"/>
<group name="SVT Group 2" domainname="example.com" uid="9d7a4b1c-9502-40e1-99b8-5e457d721930"
delete="true"/>

```

### Updating a Group

This example adds an item to the group's inbound enemies list.

```

<group name="SVT Group 2" domainname="example.com" uid="9d7a4b1c-9502-40e1-99b8-5e457d721930"
grouppriority="1" type="inbound">
  <enemy name="bubba@blockme.com"/>
</group>

```

### Assigning a Mailbox to a Group

The following example shows how to add or update a mailbox and assign it to a group.

```
<domain name="example.com">
  <mailbox name="aaron">
    <group type=manual>SVT Group 2 </group>
  </mailbox>
</domain>
```

## Outbound Settings

The following examples are for outbound IPs.

### DSN

The following is an example of settings for an Outbound IP. The Delivery Status Notification (DSN) of quarantined messages has been enabled, the maximum number of notices per hour sent to the user is set to two, and DSNs are allowed to be sent to unknown users.

```
<outbound source="10.0.0.1" gateway="" discovery="external" unrecognized="discard" dsn="true"
dsnlimit="2" odi="false" dsnunrestricted="true">
</outbound>
```

### Outbound Quarantine Access

The following example shows the outbound settings for a domain that denies access to outbound quarantined messages from the Personal Dashboard.

```
<domain name="example.com" timezone="" gateway=gateway="mailserver.example.com"
discovery="external" unrecognized="discard" odi="false" outboundaccess="false">
</domain>
```

## Encryption Settings

The following example shows encryption settings for an Outbound IP. No encryption is available between the Outbound IP and the product. The default encryption policy between the product and the Internet is to Attempt Encryption. The domain example.com is an exception. It has a policy of Required.

```
<outbound source="208.80.201.34/32" account="02d7a993-413e-45d5-a38d-5a7f19-1e3456" dns="true"
dsnlimit="3" odi="true" outboundaccess="false" sessionstls="none">
  <tlsdomains policy="available">
    <tlsdomain name="example.com" policy="required" hostname=""/>
  </tlsdomains>
</outbound>
```

## Routing and Per-Recipient Rate Limiting

The following example shows routing and per-recipient rate limit settings for an Outbound IP. It shows that each sender can email up to 40 recipients every six minutes and that the error message if this limit is exceeded is:

550 Recipient limit exceeded for this sender. Wait, don't send any more emails!

All outbound mail, with the exception of test.com, is relayed to myoutboundserver.com. Mail destined for test.com is routed to the server outbound2.com.

```
<outbound source="208.80.200.11/32" mbcleanup="0" account="a5a659b3-6901-4d8a-b231-100c0df2fcc0"
timezone="" bcc="" outbound="true" gateway="myoutboundserver.com" balanced="false"
discovery="disabled" unrecognized="accept" dsn="true" dsnlimit="unlimited" maxmsgsize="1"
spoolerduration="1" odi="true" outboundaccess="false" mphuser="unlimited" mphother="unlimited"
mphuserresponse="550 Hourly outbound rate limit exceeded = known user" mphotherresponse="550 Hourly
```



```
outbound rate limit exceeded = UNKNOWN user" rcptlimit="40" rcptlimitresponse="550 Recipient limit
exceeded for this sender. Wait, don't send any more emails!" sessiontls="available">
  <gateways>
    <gateway domain="test.com" value="outbound2.com"/>
  </gateways>
</outbound>
```

## Recipient Whitelist and Authentication

The following example shows how to add a recipient whitelist with two addresses and to turn on authentication using a verifier.

```
<outbound source="10.0.0.1" gateway="" discovery="external" unrecognized="discard" dsn="true"
dsnlimit="2" odi="false" authenticator="D2AAE5F3-B0F9-0AC9-3D22-F28C993EE270">
  <exemptrecipients>
    <exemptrecipient name="john@test.com" />
    <exemptrecipient name="george@example.com" />
  </exemptrecipients>
</outbound>
```

## CHAPTER 7 Command Line Scripting

A subset of the Email Security API consists of command line operations. As with the XML scripts, you must obtain an authentication token first. See [Obtaining and Using an Authentication Token](#). Once you have the token, you can proceed to execute any of the commands as follows:

```
curl "http://$DASHBOARD/api/<command>/<option>&token=$TOKEN&<parameters>"
```



**Note:** Executing scripts requires a system administrator role.

### Account Commands

Option	Parameter	Description	Valid Options
create		Add an account.	
	name	Name of the account.	
	contact	Account contact.	
	phone	Contact phone number.	
	country	Account country.	
	region	Region in country.	
	email	Email address of primary account contact.	Email address.
	timezone	Account time zone.	
delete		Delete the account with the given ID.	
	account	The account to delete	UID for the account.
list		List all accounts.	
	name	List all accounts starting with this name.	Any text string.

## Examples

To add an account:

```
curl "$DASHBOARD/api/account/create?token=$TOKEN&name=test&timezone=America/Los_Angeles"
```

To find the UID of an account for use in other commands:

```
curl "http://<domain>/api/account/list?token=$TOKEN&name=test"
```

To delete an account, find the UID as described above and then:

```
curl "http://$DASHBOARD/api/account/delete?token=$TOKEN&account=9F0F7DC8-D7CA-180B-26AD-A49A0F629825"
```

## Administrative User Commands

Option	Parameter	Description	Valid Options
create		Add a user to the system.	
	email	User ID.	Valid email address.
delete		Delete a user.	
	email	The user's email address.	Valid email address.
grant		Assign a role to the user.	
	email	The user's email address.	Valid email address.
	account	Grants the user administrative privileges for this account.	The account UID.
	role	Privilege level.	<b>sa:</b> system administrator <b>account:</b> account administrator <b>domain:</b> account operator <b>operator:</b> dashboard operator
list		List users.	
	role	The role for which you want the user list.	Same as above.
revoke		Revoke a user's administrative privileges.	
	email	The user's email address.	Valid email address.
	account	Revokes the user's administrative privileges for this account.	The account UID.

## Creating a User

The following command creates a new user `kim@example.com` with a password of `secret`:

```
curl "http://dashboard/api/user/create?token=$TOKEN&email=kim@example.com&password=secret"
```

If the user already exists, the command does nothing and does not update the user password. Next, assign the user an administrative role. See [Assigning User Administrative Roles](#).



**Note:** This command does not create a mailbox for the user.

## Listing Users by Role

The following command lists the users who are assigned to the specified role:

```
curl "http://dashboard/api/user/list?token=$TOKEN&role=$ROLE"
```

## Assigning User Administrative Roles

The following command grants the user `kim@example.com` the role of account administrator for the account `$ACCOUNT`.

```
curl "http://dashboard/api/user/grant?token=$TOKEN&email=kim@example.com&account=$ACCOUNT&role=account"
```

If the user does not exist, it is created and activated. You can optionally specify a password.

The account parameter is ignored for the system administrator, as permissions for this role are not specific to an account.

## Revoking User Administrative Roles

The following command revokes all administrative permissions assigned to `kim@example.com` for the account `$ACCOUNT`.

```
curl "http://dashboard/api/user/revoke?token=$TOKEN&email=kim@example.com&account=$ACCOUNT"
```

If the account is not specified, all permissions for the user are revoked from all accounts. You cannot revoke permissions for the API user.

## Deleting an Administrative User

The following command deletes the administrative user `kim@example.com`.

```
curl "http://dashboard/api/user/delete?token=$TOKEN&email=kim@example.com"
```

If the user does not exist, the command does nothing.

## Quarantine Access



**Note:** The token used to access a mailbox's quarantine must be generated using the email address and password of the mailbox. See [Obtaining and Using an Authentication Token](#).

Option	Parameter	Description	Valid Options
delete		Delete messages.	
	token	The mailbox's token.	
	id	Message identifier.	One or more IDs.
id		Retrieve a specific message.	
	token	The mailbox's token.	
list		List messages.	
	token	The mailbox's token.	
	mailbox	The user whose messages you want to list.	Valid mailbox.
	from	Starting date for the list (optional). If <from> is not specified, the list starts with the oldest message.	Date in GMT, in the format yyyy-MM-ddTHH:mm:ss.SSS). For example: 2010-04-21T13:46:01.345.
	to	Ending date for the list (optional). If <to> is not specified, the list ends with the most recent message.	Date in GMT, in the format yyyy-MM-ddTHH:mm:ss.SSS). For example: 2010-04-21T13:46:01.345.
	recent	The number of messages to list.	Integer.
release		Release messages from quarantine.	
	token	The mailbox's token.	
	id	Message identifier.	One or more IDs.
password	token	The mailbox's token.	
	password	The new password.	Minimum 6 alphanumeric characters.

### Retrieving a List of Messages

Use the following commands to retrieve a list of messages for a given user and date range.

To list quarantined messages:

```
curl "http://$DASHBOARD/api/quarantine/list?token=<token>&from=<from>&to=<to>"
```

To list delivered messages:

```
curl "http://$DASHBOARD/api/delivered/list?token=<token>&from=<from>&to=<to>"
```

Use the following commands to retrieve a list of the most recent messages for a given user.

To list the 50 most recent quarantined messages:

```
curl "http://$DASHBOARD/api/quarantine/list?token=<token>&recent=50"
```

To list the 50 most recent delivered messages:

```
curl "http://$DASHBOARD/api/delivered/list?token=<token>&recent=50"
```



**Note:** If neither <from> nor <to> is listed, all messages for the mailbox are returned. This list could be very large unless the recent token is used.

Use the following commands to retrieve a list of messages for a given user using the Admin token.

To list quarantined messages (this is an example):

```
curl
"http://svt3.redcondor.net:8080/api/quarantine/list?token=<token>&mailbox=athena@earth.svttest.net"
```

To list delivered messages (this is an example):

```
curl
"http://svt3.redcondor.net:8080/api/delivered/list?token=<token>&mailbox=athena@earth.svttest.net"
```

The following is a sample message list containing meta data for two messages:

```
<quarantine mailbox="carmenb@" timezone="America/Los_Angeles">
  <message id="20091221215511126@8f223846-d126-4ea4-8563-457fdd82d38f" received="2009-12-
  21T21:55:11.126" mailfrom="ciara123@..." recipient="carmenb@"
  messageid="&lt;579838820.20090810111615@&gt;" sender="&lt;ciara123@&gt;" subject="CIALIS SUPER
  ACTIVE+!" size="1501" sourceip="209.204.159.5" country="US" category="spam" zone="red"
  reason="1313714"/>
  <message id="20091221215639506@8f223846-d126-4ea4-8563-457fdd82d38f" received="2009-12-
  21T21:56:39.506" mailfrom="ciara123@" recipient="carmenb@"
  messageid="&lt;72280005.20090919041946@&gt;" sender="&lt;ciara123@&gt;" subject="CIALIS SUPER
  ACTIVE+!" size="1518" sourceip="209.204.159.5" country="US" category="spam" zone="red"
  reason="1313714"/>
</quarantine>
```

The mailbox is the active mailbox for the given login (usually the login email unless the user logged in with an alias).

The time zone is the effective time zone setup by the user (or domain or account). All dates returned are GMT. The time zone is reported to allow the client to convert the date/times to the user's time zone.

For each message, the following attributes are returned:

Attribute	Description
message id	An opaque ID for the message used to view, delete and release the message.

Attribute	Description
received	Date and time when the message was received.
mailfrom	The sender (from the envelope).
recipient	From the envelope, will be the same as the mailbox attribute on the quarantine element.
messageid	The MIME message ID.
sender	The MIME sender.
subject	The MIME subject.
size	The size of the message (in bytes).
sourceip	The source IP of the sender.
country	The country of the sender (geo-location based on the sender IP). For a list of country codes, see <a href="http://www.iso.org/iso/english_country_names_and_code_elements">http://www.iso.org/iso/english_country_names_and_code_elements</a> .
category	Can be any of the filtering categories supported by the application.
zone	Green, yellow or red based on the category.
reason	Internal field identifying the responsible spam filter rule.
attachment	Whether or not the message has any attachments.

## Retrieving a Message

To retrieve a specific message:

```
curl "http://$DASHBOARD/api/quarantine/<id>?token=$TOKEN"
```

Where <id> is the message identifier. For example, the id returned in the message list:

```
curl "http://$DASHBOARD/api/quarantine/20091221215511126@8f223846-d126-4ea4-8563-457fdd82d38f?token=$TOKEN"
```

## Releasing a Message

To release a specific message:

```
curl "http://$DASHBOARD/api/quarantine/release?token=$TOKEN&id=<id>"
```

Where <id> is the message identifier. For example, the id returned in the message list:

```
curl "http://example.acme.net/api/quarantine/release?token=$TOKEN&id=20100415235914560@8f223846-d126-4ea4-8563-457fdd82d38f"
```

To release multiple messages :

```
curl "http://$DASHBOARD/api/quarantine/release?token=<token>&id=<id1>&id=<id2>"
```

Where <idx> is the message identifier id.

To release delivered messages:

```
curl "http://$DASHBOARD/api/delivered/release?token=<token>&id=<id1>&id=<id2>"
```

Where <idx> is the message identifier id.

## Deleting a Message

To delete a specific message:

```
curl "http://$DASHBOARD/api/quarantine/delete?token=$TOKEN&id=<id>"
```

For example:

```
curl "http://example.acme.net/api/quarantine/delete?token=$TOKEN&id=20100516183935258@8f223846-d126-4ea4-8563-457fdd82d38f"
```

To delete multiple messages with one command:

```
curl "http://$DASHBOARD/api/quarantine/delete?token=<token>&id=<id1>&id=<id2>"
```

## Changing a Password

If login authentication is local to the appliance, you can change a password by entering the following:

```
curl "http://$DASHBOARD/api/password?token=<token>&password=xyz"
```

This command changes the password for the user identified by the token (acquired using the login or token API calls).

## Domain Commands

Use the following commands to view, create, update and delete domains.



**Note:** The operations that can be performed with this command line API are limited in functionality. Not all domain settings can be configured with this API. The XML API must be used instead.

Option	Parameter	Description	Valid Options
create		Add a domain.	
	name	Name of the domain to create. (Required)	
	account	The account to contain the domain. (Required)	Account UID.
	property	Settings to apply to the domain. Settings not specified are assigned default values.	For a list of valid settings see <a href="#">Domain Settings</a> .



Option	Parameter	Description	Valid Options
delete		Delete the domain with the given ID.	
	name	Name of the domain to delete. (Required)	
	account	The account that contains the domain. (Required)	Account UID.
list		List domains.	
	name	List all domains starting with this name.	Any text string.
	account	The account that contains the domains.	Account UID.
update		Update domain settings.	
	name	Name of the domain to update. (Required)	
	account	The account that contains the domain.	Account UID.
	property	Settings to update. Settings not specified are not updated.	For a list of valid settings see <a href="#">Domain Settings</a> .

## Listing Domains

To list domains starting with the given prefix in the specified account:

```
/api/domain/list?token=<token>&name=<prefix>&account=<uid>
```

If no account is specified, all domains within the brand are listed that start with the given prefix. If no prefix is specified, all domains in the brand are listed.

Example:

```
http://svt3.redcondor.net/api/domain/list?token=$TOKEN&name=str?account=4719F67E-8854-F6EA-0997-40976869F3A6
```

## Creating a Domain

To create a domain:

```
/api/domain/create?token=<token>&name=<name>&account=<uid>&<property>=<value>...
```

Example:

```
http://svt3.redcondor.net/api/domain/create?token=$TOKEN&name=test3.com?account=4719F67E-8854-F6EA-0997-40976869F3A6&unrecognized=bounce
```

## Deleting a Domain

To delete a domain:

```
/api/domain/delete?token=<token>&name=<name>&account=<uid>
```

Example:

```
http://svt3.redcondor.net/api/domain/delete?token=$TOKEN&name=test3.com?account=4719F67E-8854-F6EA-0997-40976869F3A6
```

## Updating Domain Settings

To update the settings in a domain:

```
/api/domain/update?token=<token>&name=<name>&<property>=<value>...
```

Example:

```
http://svt3.redcondor.net/api/domain/update?token=$TOKEN&name=test3.com&account=4719F67E-8854-F6EA-0997-40976869F3A6&discovery=rcpt&timezone=america/Los_Angeles
```

## Outbound IP Commands

Use the following commands to create, update and delete outbound IPs or shared outbound IPs.



**Note:** The operations that can be performed with this command line API are limited in functionality. Not all settings for shared outbound IPs can be configured with this API. The XML API must be used instead.

Option	Parameter	Description	Valid Values
create		Add a outbound IP.	
	name	Single IP or IP range (not shared)	IP address in CIDR notation
	account	The account that will use the new IP (Required)	Account UID
	service or id	Choose a valid value. (shared outbound only)	- Office365 (id=1) - Google Apps (id=2)
delete		Delete an outbound IP.	
	name	Single IP or IP range or shared outbound IP (Required)	IP in CIDR notation or _port_ outbound.<id>.<port#>

Option	Parameter	Description	Valid Values
update		Update an outbound IP.	
	name	Single IP or IP range or shared outbound IP to update (Required)	IP in CIDR notation or _port_ outbound.<id>.<port#>
	account	The new account to contain the outbound IP or shared outbound IP.	Account UID
	settings	Settings to update. Settings not specified are not updated.	For a list of valid settings see <a href="#">Domain Settings</a>

## Creating an Outbound IP

To create a outbound IP or IP range:

```
/api/domain/create?token=<token>&name=<ip_or_ip_range>&account=<uid>
```

Example:

```
http://example.redcondor.net/api/domain/create?token=$TOKEN&name=10.11.2.3&account=4719F67E-8854-F6EA-0997-40976869F3A6
```

To create a shared outbound IP:

```
/api/domain/create?token=<token>&account=<uid>&<service>=<value>
```

or

```
/api/domain/create?token=<token>&account=<uid>&<id>=<value>
```

Example:

```
https://example.redcondor.net/api/domain/shared/create?token=$token&account=$account_uid&service=google%20apps
```

or

```
https://example.redcondor.net/api/domain/shared/create?token=$token&id=1&account=2d764e09-2d99-4614-b0ec-fb5cf22723e3
```

## Deleting an Outbound IP

To delete an outbound IP:

```
/api/domain/delete?token=<token>&name=<ip_or_ip_range>
```

Example:

```
http://example.redcondor.net/api/domain/delete?token=$TOKEN&name=10.11.2.3
```

To delete a shared outbound IP:

```
/api/domain/shared/delete?token=<token>&name=_port_outbound.<id>.<port>
```

**Example:**

```
http://example.redcondor.net/api/domain/shared/delete?token=$TOKEN&name=_port_outbound.1.31387
```

**Updating an Outbound IP**

To update the settings for an outbound IP:

```
/api/domain/update?token=<token>&name=<ip_or_ip_range>&<property>=<value>...
```

**Example:**

```
http://example.redcondor.net/api/domain/update?token=$TOKEN&name=10.11.2.3&retainblocked=true&retaindelivered=false
```

To update the settings for a shared outbound IP:

```
/api/domain/shared/update?token=<token>&name=_port_outbound.<id>.<port>&<property>=<value>...
```

**Example:**

```
http://example.redcondor.net/api/domain/shared/update?token=$TOKEN&name=_port_outbound.1.37169&retainblocked=true&retaindelivered=false
```

**Mailbox Commands**

Use the following commands to view, create, update and delete mailboxes.



**Note:** The operations that can be performed with this command line API are limited in functionality. Not all mailbox settings can be configured with this API. The XML API must be used instead.

Option	Parameter	Description	Valid Options
create		Add a mailbox.	
	email	Name of the mailbox to create. The mailbox is added to the domain specified in the email address. (Required)	Email address.
	property	Settings to apply to the mailbox. Settings not specified are assigned default values.	For a list of valid settings see <a href="#">Mailbox Settings</a> .
delete		Delete a mailbox.	
	email	Name of the mailbox to delete. (Required)	Email address.

Option	Parameter	Description	Valid Options
list		List mailboxes or settings.	
	domain	List all mailboxes in this domain.	Valid domain.
	email	List the settings for this mailbox.	Email address.
update		Update mailbox settings.	
	email	Name of the mailbox to update. (Required)	Email address.
	property	Settings to update. Settings not specified are not updated.	For a list of valid settings see <a href="#">Mailbox Settings</a> .

## Listing Mailboxes

To list all mailboxes in a domain:

```
/api/mailbox/list?domain=<domain>
```

Example:

```
http://svt3.redcondor.net/api/mailbox/list?token=$TOKEN&domain=svt3.com
```

To list the settings for a particular mailbox:

```
/api/mailbox/list?email=<email>
```

Example:

```
http://svt3.redcondor.net/api/mailbox/list?token=$TOKEN&email=john@svt3.com
```

## Creating a Mailbox

To create a mailbox:

```
/api/domain/create?token=<token>&email=<name>
```

Example:

```
http://svt3.redcondor.net/api/mailbox/create?token=$TOKEN&email=john@test3.com&status=active
```

## Deleting a Mailbox

To delete a mailbox:

```
/api/mailbox/delete?token=<token>&email=<name>
```

Example:

```
http://svt3.redcondor.net/api/mailbox/delete?token=$TOKEN&email=sam@test3.com
```

## Mailboxes - Update

To update mailbox settings:

```
/api/mailbox/update?token=<token>&email=<name>&<property>=<value>...
```

Example:

```
http://svt3.redcondor.net/api/mailbox/update?token=$TOKEN&email=sara@test3.com&status=unprotected
```

## Mailbox Alias Commands

Use the following commands to view, create, and delete mailbox aliases.



**Note:** The operations that can be performed with this command line API are limited in functionality. Not all mailbox alias settings can be configured with this API. The XML API must be used instead.

Option	Parameter	Description	Valid Options
create		Add a mailbox alias.	
	email	Primary email address. (Required)	Email address.
	alias	Alias email address. (Required)	Email address.
delete		Delete a mailbox alias.	
	email	Primary email address. (Required)	Email address.
	alias	Alias email address. (Required)	Email address.
list		List mailbox aliases.	
	email	List the aliases for this mailbox.	Email address.

## Listing Mailbox Aliases

To list all aliases of a mailbox:

```
/api/alias/list?email=<name>
```

Example:

```
http://svt3.redcondor.net/api/alias/list?token=$TOKEN&email=helen@svt3.com
```

## Creating Mailbox Aliases

To create an alias for a mailbox:

```
/api/alias/create?token=<token>&email=<name>&alias=<alias>
```

Example:

```
http://svt3.redcondor.net/api/alias/create?token=$TOKEN&email=john@test3.com&alias=sara@test3.com
```

In this example the alias is sara@test3.com:

```
http://svt3.redcondor.net/api/alias/create?token=$TOKEN&email=john@test3.com&alias=sara
```

In this example the alias is in another domain, svt3.com, which must have already been set up:

```
http://svt3.redcondor.net/api/alias/create?token=$TOKEN&email=john@test3.com&alias=sara@svt3.com
```

## Deleting a Mailbox Alias

To delete an alias for a mailbox:

```
/api/alias/delete?token=<token>&email=<name>&alias=<alias>
```

Example:

```
http://svt3.redcondor.net/api/alias/delete?token=$TOKEN&email=john@test3.com&alias=sara@test3.com
```

## Verifier Commands

A verifier is an object used in domain configuration. It consists of settings used for communicating with the verification server. Verifiers define a method for determining the validity of an email address and/or authenticating a user.

Option	Parameter	Description	Valid Options
create		Adds a verifier.	
	name	Name of the verifier.	Any text string.
	account	Account in which to create the verifier.	UID of the account (empty makes it a system-wide verifier).
	xml	XML verifier definition.	
delete		Deletes a verifier.	
	UID	UID of the verifier to delete.	Valid UID.
list		Lists all verifiers.	
list	account	Lists of all verifiers in an account.	Account UID.
list	UID	Returns the verifier contents in XML format.	Valid UID.
update		Modifies a verifier.	
	UID	UID of the verifier to update.	Valid UID.
	xml	XML verifier definition.	

## Listing Verifiers

To download a list of all verifiers in a brand (for example, xxx.acme.net) with complete details:

```
curl "http://$DASHBOARD/api/verifier/list?token=$TOKEN"
```

The following example downloads all verifiers in the account \$ACCOUNT:

```
curl "http://$DASHBOARD/api/verifier/list?token=$TOKEN&account=$ACCOUNT"
```

Where "\$ACCOUNT" is the UID of the account.

## Creating a Verifier

You can create a verifier in one of three ways:

- Using an XML parameter:

```
curl "http://$DASHBOARD/api/verifier/create?token=$TOKEN&name=test&account=$ACCOUNT&xml=<foo/>"
```

Where <foo/> is the XML definition of the verifier.

- Using a data file:

```
curl -F "data=@verifier.xml"
"http://$DASHBOARD/api/verifier/create?token=$TOKEN&name=test&account=$ACCOUNT"
```

Where verifier.xml is the datafile containing the definition of the verifier.

- Streaming the XML definition:

```
echo "<foo/>" | curl -H 'Content-type: text/xml' --data-binary @-
"$DASHBOARD/api/verifier/create?token=$TOKEN&name=test&account=$ACCOUNT"
```

Where <foo/> is the XML definition of the verifier.

The following is a sample XML definition of a verifier:

```
<Vrfy version="101.3807">
  <MetaData>
    <Editable>true</Editable>
  </MetaData>
  <LDAP defaults="ActiveDirectory">
    <Host secure="false">postal.acme.com</Host>
    <HostListOrder>Shuffle</HostListOrder>
    <Timeout>5</Timeout>
  </LDAP>
</Vrfy>
```

## Modifying a Verifier

You can modify the name or XML definition. When downloading the configuration for a domain referencing a verifier, the verifier definition will also be returned and can be modified and uploaded again.

The following example changes the XML definition to <foo/>:

```
curl "http://$DASHBOARD/api/verifier/update?token=$TOKEN&uid=xxxxxxx&&xml=<foo/>"
```

Where xxxxxx is the UID of the verifier, and <foo/> is the new XML definition.



The following example changes a verifier by using a data file:

```
curl -F "data=@vrfy_xml_file" "http://$brand/api/verifier/update?token=$token&uid=$vrfy_uid"
```

## Deleting a Verifier

To delete a verifier:

```
curl "http://$DASHBOARD/api/verifier/delete?token=$TOKEN&uid=xxxxxxx"
```

Where xxxxxx is the UID of the verifier.

## Content Filter Commands

Content filters are used in keyword filtering to detect messages containing specific words in the headers, message body, and plain text attachments. Other types of attachments are not filtered. Primarily used as a security measure to prevent data leaks in outgoing mail, administrators create one or more content filters in an account, then activate filters on individual domains or outbound IPs as needed.

Administrators might create multiple content filters for specific content. For example, you might create content filters for financial terms, discrimination, profanity, or sexual content. Individual domains could use the combination of content filters according to their need.

You can use A-Z, a-z, 0-9, hyphen(-), or underscore(\_) to match words and phrases. Keywords are not case sensitive.

Option	Parameter	Description	Valid Options
create		Add a content filter to the system.	
	name	Name of the content filter.	Any text string.
	account	Creates a content filter for a specific account.	UID of the account (empty makes it a system-wide content filter), rule content.
	encryptRemoveSubject	Whether to remove the filter words from the message subject.	True or False. This should only be used with a Subject header rule.
	dlpCustom	Enables/disables use of a content filter by the DLP engine in outbound filtering.	True or False.
delete		Delete a content filter.	
	UID	UID of the content filter to delete.	

Option	Parameter	Description	Valid Options
list		List all content filters.	
	account	List of all content filters in an account.	Account UID.
	UID	Return the content filter rules in XML format.	Valid UID.
update		Modify a content filter.	
	UID	UID of the content filter to update.	Valid UID.
	name	Name of the content filter.	Any text string.
	data	Adds and removes rules in a content filter.	Rule content.
	encryptRemoveSubject	Whether to remove the filter words from the message subject.	True or False. This should only be used with a Subject header rule.
	dlpCustom	Enables/disables use of a content filter by the DLP engine in outbound filtering.	True or False.

## Content Filter Rules

The content filter consists of one or more rules. In each rule you can select whether to filter the whole message and/or one or more headers. A content filter set to Accept or Block is run after the antivirus and Friends and Enemies filters, and before all other filters.

The syntax for a rule is as follows:

```
{"parts":["HEADER","TEXT"],"filters":["bar","foo"],"headers":["Subject:","From:"]}
```

Parameter	Description	Valid Options
"parts"	Which part of the message to check.	"HEADER" - Specify which headers in "headers" (see below) "TEXT" - Search the message body. Enclose options in double quotes and separate them with a comma.

Parameter	Description	Valid Options
"filters"	What to look for in the message.	List specific words, numbers, or regular expressions. Enclose options in double quotes and separate them with a comma.
"headers"	Which headers to check.	Only include this if one of the "parts" is "HEADER" Enclose options in double quotes and separate them with a comma.

- Each list is enclosed in square brackets []
- Each rule is enclosed in curly brackets {}
- The set of rules is enclosed square brackets []
- The list of rules is comma separated

Here is an example of several rules in one content filter:

```
{ "parts": ["TEXT"], "filters": ["\\b\\d{1,3}\\b\\.\\d{1,3}\\b\\.\\d{1,3}\\b\\.\\d{1,3}\\b"],
  "parts": ["TEXT"], "filters": ["\\w\\btest2"]},
{ "parts": ["HEADER"], "filters": "bar", "foo", "headers": ["Subject:"]},
{ "parts": ["HEADER", "TEXT"], "filters": ["marytest"], "headers": ["Subject:"]}]
```

## Listing Content Filters

To download a list of all content filters in a brand with complete details:

```
curl "http://$DASHBOARD/api/contentfilter/list?token=$TOKEN"
```

The following example downloads all content filters in the account \$ACCOUNT:

```
curl "http://$DASHBOARD/api/contentfilter/list?token=$TOKEN&account=$ACCOUNT"
```

## Downloading a Content Filter

To download all of the content filters for a brand:

```
curl "http://$DASHBOARD/api/contentfilter/list?token=$TOKEN"
```

To download all the content filters for an account:

```
curl "http://$DASHBOARD/api/contentfilter/list?token=$TOKEN&account=A5A659B3-6901-4D8A-B231-100C0DF2FCC0"
```

To download the rules for the content filter UID in XML format:

```
curl "http://$DASHBOARD/api/contentfilter/52BD2714-A881-4772-ACF2-EFB82CF53BD7?token=$TOKEN"
```

## Creating a Content Filter

You can use A-Z, a-z, 0-9, hyphen(-), or underscore(\_) to match words. Keywords are not case-sensitive.

To create a content filter using a data file:

```
curl -F "data=@contentfilter.txt"
"http://$DASHBOARD/api/contentfilter/create?token=$TOKEN&name=test&account=$ACCOUNT"
```

Where `contentfilter.txt` is the datafile containing the list of words formatted using the syntax rules described above.

To create a content filter by streaming words:

```
echo '{"parts":["HEADER","TEXT"],"filters":["bar","foo"],"headers":{"Subject:","From:"}}' | curl -
H 'Content-type: text/plain' --data-binary @-
"$DASHBOARD/api/contentfilter/create?token=$TOKEN&name=test&account=$ACCOUNT"
```

Where `'{"parts":["HEADER","TEXT"],"filters":["bar","foo"],"headers":{"Subject:","From:"}}'` is one rule.

## Modifying a Content Filter

You can modify the name and definition, or reassign the content filter to a different account. When downloading the configuration for a domain referencing a content filter, the content filter definition will also be returned and can be modified and uploaded again.

The following example reads from the text file `contentfilter01.txt` and replaces the content filter identified by the given UID with the contents of the file:

```
curl -F "data=@contentfilter01.txt" "http://$DASHBOARD/api/contentfilter/update?&uid=FFF1DAFF-8BBC-
4C17-953B-287423F52312&token=$TOKEN"
```

The following example changes the name of the content filter specified with the token to `contentfilter02`:

```
curl "http://$DASHBOARD/api/contentfilter/update?&token=$TOKEN&uid=FC9DBB74-16D9-4CA1-9704-
DFF62D744705&name=contentfilter02"
```

The following example updates the content filter by replacing the contents with the rule `'{"parts":["HEADER","TEXT"],"filters":["bar","foo"],"headers":{"Subject:","From:"}}'`:

```
echo '{"parts":["HEADER","TEXT"],"filters":["bar","foo"],"headers":{"Subject:","From:"}}' | curl -
H 'Content-type: text/plain' --data-binary @-
"$DASHBOARD/api/contentfilter/update?token=$TOKEN&account=A5A659B3-6901-4D8A-B231-
100C0DF2FCC0&uid=47A0E318-1AA2-4F54-B825-D3464C74288E"
```

The following example enables `dlpCustom` and disables `encryptRemoveSubject`:

```
curl
"https://$DASHBOARD/api/contentfilter/update?token=bWFYeW1AcnVkY29uZG9yLmNvbQAAAVTVjp18n3eU8vKHHW8G
xeb6KSElmcFMtpI&uid=8087f625-e5a6-47b2-8695-56a569087872&dlpCustom=true&encryptRemoveSubject=false"
```

## Deleting a Content Filter

To delete a content filter:

```
curl "http://$DASHBOARD/api/contentfilter/delete?token=$TOKEN&uid=FFF1DAFF-8BBC-4C17-953B-
287423F52312"
```

## Reporting

You can generate a report that lists each account, the domains and groups within the account, and the mailbox count for each domain.

To retrieve the report:

```
curl "http://brand/api/manage/report?token=$token&report=true"
```

Sample output:

```
<report account="11" domain="11" outbound="3" mbactive="6" mbinactive="3" mbunprotected="1">
  <accounts>
    <account name="DAPI TET" uid="2586c44c-f631-4e17-a3c0-0f813babb520">
      <domains>
        <domain name="testgroup2.svttest.net" mbactive="0" mbinactive="0" mbunprotected="0"/>
        <domain name="testgroup3.svttest.net" mbactive="0" mbinactive="0" mbunprotected="0"/>
        <domain name="testgroup.svttest.net" mbactive="0" mbinactive="0" mbunprotected="0"/>
      </domains>
    </account>
    <account name="Svt2 Account" uid="1252ad2c-4266-496c-9d21-8d67d7bff4ab">
      <domains>
        <domain name="futz.svttest.net" mbactive="3" mbinactive="1" mbunprotected="0"/>
        <domain name="source.org" mbactive="0" mbinactive="0" mbunprotected="0"/>
        <domain name="target.org" mbactive="2" mbinactive="0" mbunprotected="0"/>
      </domains>
    </account>
    <account name="DAPI Mozdom" uid="2586c44c-f631-4e17-a3c0-0f813babb520">
      <domains>
        <domain name="decode.com" mbactive="0" mbinactive="0" mbunprotected="0">
          <groups>
            <group name="decode group 1"/>
            <group name="decode group 2"/>
            <group name="group1"/>
            <group name="nuder group test"/>
          </groups>
        </domain>
        <domain name="mozdom.com" mbactive="1" mbinactive="0" mbunprotected="0"/>
        <domain name="mozdom.svttest.net" mbactive="0" mbinactive="0" mbunprotected="0">
          <groups>
            <group name="SVT Group"/>
            <group name="SVT Group 2"/>
            <group name="SVT Group 3"/>
          </groups>
        </domain>
        <domain name="testgroup.svttest.net" mbactive="0" mbinactive="0" mbunprotected="0"/>
      </domains>
    </account>
  </accounts>
</report>
```

## CHAPTER 8 Portal API

Calls to RESTful services are done through URLs. The base URL for the MWD service is:

```
https://portal.edgewave.com:8005/mwd
```

In the following examples:

- `{base}` means the base URL; do NOT include the curly-braces.
- `{params}` are in the form `param1=value1&param2=value2...`; do not include the curly-braces.
- Where the example URL says (resellerid), DO include the parentheses.

There are two HTTP headers that have to be set:

- **Authorization** - The Authorization header should hold the value of the token received from a token request.
- **Content-Type** - The Content-Type should be set to `application/json`.

Unless otherwise stated below, the HTTP successful response code is "200 OK."

The following are general error codes that can appear:

- 409 Token has expired
- 400 Bad request

### Token Request

Description	Authentication is required for all Portal API requests. Use this URI to obtain a token authorizing you to access the service.
URI	<code>{base}/token?user={username}&amp;password={password}</code>
Parameters	The <code>{username}</code> and <code>{password}</code> are the ones you use to log in on the portal. Do not include the curly-braces.
HTTP verb	POST

Example	<p>Suppose your portal login is me@acme.com and your password is abc123. To get a token, the full URL is:</p> <pre>https://portal.acme.com:8005/mwd/token?user=me@acme.com &amp;password=abc123</pre>
Result	If the call is successful, a token string is returned. Use the token in the Authorization header for subsequent requests.
Error codes	<p>401 User Password does not match</p> <p>401 User not found</p>

## Get Resellers Request

Description	Use this URI to get a list of the resellers linked to your distributor account.
URI	{base}/resellers
Parameters	None
HTTP verb	GET
Example	https://portal.acme.com:8005/mwd/resellers
Result	<pre>[ {   Name: "Reseller1 Account"   ID: "247dba33-1fdd-44a3-ae00-3e6132ca3547"   Dashboard: "test1.griffin.net"   NumberOfClients: 46 } {   Name: "Reseller2 Account"   ID: "76cc6dec-6782-4e7e-a9ad-97f08e45b215"   Dashboard: "test1.duncan.net"   NumberOfClients: 6 } ]</pre>
Error codes	<p>409 Token has expired</p> <p>400 Bad request</p>

## Get Reseller Details Request

Description	Use this URI to view the account details of a particular reseller.
URI	{base}/resellers/{resellerid}
Parameters	The <code>resellerid</code> is the reseller's account ID as returned by the Get Resellers request. The parentheses are required.

HTTP verb	GET
Example	<code>https://portal.acme.com:8005/mwd/resellers/(2d6d1f64-430c-4331-ae71-a88a2ea9b3f8)</code>
Result	<pre>{   "AccountName": "test0528",   "AccountID": "2d6d1f64-430c-4331-ae71-a88a2ea9b3f8",   "Address": "",   "City": "",   "State": "California",   "Zip": "",   "Country": "United States",   "FirstName": "Joe",   "LastName": "Tester",   "Email": "tester@acme.com",   "Phone": "6195552222",   "Dashboard": "example.acme.net",   "ResellerDashboard": "example.acmeresellers.net",   "NumberOfClients": 1 }</pre>
Error codes	<p>409 Token has expired</p> <p>400 Bad request</p>

## Delete Reseller Request

Description	Use this URI to remove a reseller.
URI	<code>{base}/resellers/{resellerid}</code>
Parameters	The <code>resellerid</code> is the reseller's account ID as returned by the Get Resellers request. The parentheses are required.
HTTP verb	DELETE
Example	<code>https://portal.acme.com:8005/mwd/resellers/(247dba33-1fdd-44a3-ae00-3e6132ca3547)</code>
Result	This command disables and deactivates the reseller, and disables the accounts of the reseller's clients.
Error codes	<p>409 Token has expired</p> <p>400 Bad request</p>

## Get Reseller Clients Request

Description	Use this URI to get a list of a reseller's clients.
URI	<code>{base}/resellers/{resellerid}/clients</code>
Parameters	The <code>resellerid</code> is the reseller's account ID as returned by the Get Resellers request. The parentheses are required.



HTTP verb	GET
Example	<code>https://portal.acme.com:8005/mwd/resellers/(247dba33-1fdd-44a3-ae00-3e6132ca3547)/clients</code>
Result	<pre>[   {     Name: "Account 1"     ID: "e7d6dca3-eb8f-4876-9770-447c3479f77c"     Dashboard: "test1.acme.net"   },   {     Name: "Account2"     ID: "25c1b7e1-8a30-4786-807d-d6f1cc59af47"     Dashboard: "test1.fudd.net"   },   {     Name: "Account3"     ID: "5f740763-9b54-4e8a-8bf3-ff3b763af7b2"     Dashboard: "test1.rrunner.net"   } ]</pre>
Error codes	<p>409 Token has expired</p> <p>400 Bad request</p>

## Create Reseller Request

Description	Use this URI to create a reseller.
URI	<code>{base}/resellers/create/{params}</code>
Parameters	<p><code>{params}</code> is in the normal query string format, <code>param1=value1&amp;param2=value2...</code></p> <p>Acceptable params are:</p> <ul style="list-style-type: none"> <li>• name - the account name</li> <li>• email - primary contact email</li> <li>• firstname - first name of primary contact</li> <li>• lastname - last name of primary contact</li> <li>• address - street address for the reseller account</li> <li>• city - city for the reseller account</li> <li>• state - state for the reseller account</li> <li>• country - country for the reseller account</li> </ul>

	<ul style="list-style-type: none"> <li>zip - zip code for reseller account</li> </ul> <p>Quotation marks are required around parameter values with spaces.</p>
HTTP verb	POST
Example	<code>https://portal.acme.com:8005/mwd/resellers/create/name="A Made up Reseller"&amp;address="27 Square St."&amp;email=bigshot@fakemail.com</code>
Result	<pre>{   "AccountID": "a7241c61-2a4c-4a84-bd14-ded1dddcc186",   "AccountName": "A Made up Reseller",   "Address": "27 Square St.",   "City": "Acme",   "Country": "United States",   "Dashboard": "mystore.acme.com",   "Email": "bigshot@fakemail.com",   "FirstName": "Joe",   "LastName": "Tester",   "Phone": "123-4567",   "State": "California",   "Zip": "92128",   "NumberOfClients": 1 }</pre> <p>Note: Unspecified parameters are populated with values from the distributor account. Incorrect values can be changed with the Edit Reseller request.</p>
Error codes	<p>409 Token has expired</p> <p>400 Bad request</p>

## Edit Reseller Request

Description	Use this URI to edit a reseller.
URI	<code>{base}/resellers/{resellerid}/{params}</code>
Parameters	<p><code>{params}</code> is in normal query string format: <code>param1=value1&amp;param2=value2...</code></p> <p>The acceptable params for editing a reseller are the same as the acceptable params for creating a reseller. See the Create Reseller request.</p>
HTTP verb	PUT
Example	<code>https://portal.tutone.com:8005/mwd/resellers/(a7241c61-2a4c-4a84-bd14-ded1dddcc186)/firstname=Jenny&amp;lastname=Song&amp;phone=867-5309</code>

Result	<pre>{   "AccountID": "a7241c61-2a4c-4a84-bd14-ded1dddcc186",   "AccountName": "Tommy Tutone",   "Address": "27 Square St.",   "City": "sd",   "Country": "United States",   "Dashboard": "mystore.acme.net",   "Email": "bigshot@fakemail.com",   "FirstName": "Jenny",   "LastName": "Song",   "Phone": "867-5309",   "State": "California",   "Zip": "92128",   "NumberOfClients": 1 }</pre>
Error codes	<p>409 Token has expired</p> <p>400 Bad request</p>

## Move Client Request

Description	Use this URI to move an account from one reseller to another.
URI	{base}/resellers/(resellerid)/clients/(clientid)/reseller=(reseller2id)
Parameters	<ul style="list-style-type: none"> <li><code>clientid</code> is the client's account ID as returned by the Get Reseller Clients request</li> <li><code>resellerid</code> is the account ID of the source reseller, as returned by the Get Resellers request</li> <li><code>reseller2id</code> is the account ID of the destination reseller</li> </ul> <p>DO include the parentheses.</p> <p>The source and target resellers must have their accounts on the same dashboard.</p>
HTTP verb	POST
Example	https://portal.acme.com:8005/mwd/resellers/(6657fdc7-b02d-42f4-bf01-87838edfa2ca)/clients/(0d645b70-f316-41cd-8455-f5679800cfee)/reseller=(1d44a246-82dd-4783-83ab-7ea47bc591c1)
Result	301 Client moved
Error codes	409 Different dashboards: Client is on test1.acme.net but reseller uses test2.acme.net

## Associate Client Request

Description	Use this URI to associate a distributor's client with one of the distributor's resellers.
URI	{base}/clients/(clientid)/reseller=(resellerid)
Parameters	<ul style="list-style-type: none"> <li><code>clientid</code> is the client's account ID found in the URL of the Account page on the dashboard</li> </ul>

	<ul style="list-style-type: none"><li><code>resellerid</code> is the account ID of the reseller as returned by the Get Resellers request</li></ul> <p>The target reseller and the client must already have their accounts on the same dashboard.</p>
HTTP verb	POST
Example	<code>https://portal.acme.com:8005/mwd/clients/(92DEEACC-025A-4952-B916-2A26A44544B2)/reseller=(6657fdc7-b02d-42f4-bf01-87838edfa2ca)</code>
Result	200 OK
Error codes	404 Account not found

## APPENDIX A Supported Time Zones

The table below shows the supported time zones:

Africa/Abidjan	America/North_Dakota/Center	Australia/Lindeman
Africa/Accra	America/North_Dakota/New_Salem	Australia/Lord_Howe
Africa/Addis_Ababa	America/Panama	Australia/Melbourne
Africa/Algiers	America/Pangnirtung	Australia/North
Africa/Asmara	America/Paramaribo	Australia/NSW
Africa/Asmera	America/Phoenix	Australia/Perth
Africa/Bamako	America/Port_of_Spain	Australia/Queensland
Africa/Bangui	America/Port-au-Prince	Australia/South
Africa/Banjul	America/Porto_Acre	Australia/Sydney
Africa/Bissau	America/Porto_Velho	Australia/Tasmania
Africa/Blantyre	America/Puerto_Rico	Australia/Victoria
Africa/Brazzaville	America/Rainy_River	Australia/West
Africa/Bujumbura	America/Rankin_Inlet	Australia/Yancowinna
Africa/Cairo	America/Recife	Brazil/Acre
Africa/Casablanca	America/Regina	Brazil/DeNoronha
Africa/Ceuta	America/Resolute	Brazil/East
Africa/Conakry	America/Rio_Branco	Brazil/West
Africa/Dakar	America/Rosario	Canada/Atlantic
Africa/Dar_es_Salaam	America/Santiago	Canada/Central
Africa/Djibouti	America/Santo_Domingo	Canada/Eastern

Africa/Douala	America/Sao_Paulo	Canada/East-Saskatchewan
Africa/El_Aaiun	America/Scoresbysund	Canada/Mountain
Africa/Freetown	America/Shiprock	Canada/Newfoundland
Africa/Gaborone	America/St_Johns	Canada/Pacific
Africa/Harare	America/St_Kitts	Canada/Saskatchewan
Africa/Johannesburg	America/St_Lucia	Canada/Yukon
Africa/Kampala	America/St_Thomas	Chile/Continental
Africa/Khartoum	America/St_Vincent	Chile/EasterIsland
Africa/Kigali	America/Swift_Current	Etc/Greenwich
Africa/Kinshasa	America/Tegucigalpa	Etc/UCT
Africa/Lagos	America/Thule	Etc/Universal
Africa/Libreville	America/Thunder_Bay	Etc/UTC
Africa/Lome	America/Tijuana	Etc/Zulu
Africa/Luanda	America/Toronto	Europe/Amsterdam
Africa/Lubumbashi	America/Tortola	Europe/Andorra
Africa/Lusaka	America/Vancouver	Europe/Athens
Africa/Malabo	America/Virgin	Europe/Belfast
Africa/Maputo	America/Whitehorse	Europe/Belgrade
Africa/Maseru	America/Winnipeg	Europe/Berlin
Africa/Mbabane	America/Yakutat	Europe/Bratislava
Africa/Mogadishu	America/Yellowknife	Europe/Brussels
Africa/Monrovia	Antarctica/Casey	Europe/Bucharest
Africa/Nairobi	Antarctica/Davis	Europe/Budapest
Africa/Ndjamena	Antarctica/DumontDUrville	Europe/Chisinau
Africa/Niamey	Antarctica/Mawson	Europe/Copenhagen

Africa/Nouakchott	Antarctica/McMurdo	Europe/Dublin
Africa/Ouagadougou	Antarctica/Palmer	Europe/Gibraltar
Africa/Porto-Novo	Antarctica/Rothera	Europe/Guernsey
Africa/Sao_Tome	Antarctica/South_Pole	Europe/Helsinki
Africa/Timbuktu	Antarctica/Syowa	Europe/Isle_of_Man
Africa/Tripoli	Antarctica/Vostok	Europe/Istanbul
Africa/Tunis	Arctic/Longyearbyen	Europe/Jersey
Africa/Windhoek	Asia/Aden	Europe/Kaliningrad
America/Adak	Asia/Almaty	Europe/Kiev
America/Anchorage	Asia/Amman	Europe/Lisbon
America/Anguilla	Asia/Anadyr	Europe/Ljubljana
America/Antigua	Asia/Aqtou	Europe/London
America/Araguaina	Asia/Aqtobe	Europe/Luxembourg
America/Argentina/Buenos_Aires	Asia/Ashgabat	Europe/Madrid
America/Argentina/Catamarca	Asia/Ashkhabad	Europe/Malta
America/Argentina/ComodRivada via	Asia/Baghdad	Europe/Mariehamn
America/Argentina/Cordoba	Asia/Bahrain	Europe/Minsk
America/Argentina/Jujuy	Asia/Baku	Europe/Monaco
America/Argentina/La_Rioja	Asia/Bangkok	Europe/Moscow
America/Argentina/Mendoza	Asia/Beirut	Europe/Nicosia
America/Argentina/Rio_Gallegos	Asia/Bishkek	Europe/Oslo
America/Argentina/San_Juan	Asia/Brunei	Europe/Paris
America/Argentina/Tucuman	Asia/Calcutta	Europe/Podgorica
America/Argentina/Ushuaia	Asia/Choibalsan	Europe/Prague
America/Aruba	Asia/Chongqing	Europe/Riga
America/Asuncion	Asia/Chungking	Europe/Rome
America/Atikokan	Asia/Colombo	Europe/Samara

America/Atka	Asia/Dacca	Europe/San_Marino
America/Bahia	Asia/Damascus	Europe/Sarajevo
America/Barbados	Asia/Dhaka	Europe/Simferopol
America/Belem	Asia/Dili	Europe/Skopje
America/Belize	Asia/Dubai	Europe/Sofia
America/Blanc-Sablon	Asia/Dushanbe	Europe/Stockholm
America/Boa_Vista	Asia/Gaza	Europe/Tallinn
America/Bogota	Asia/Harbin	Europe/Tirane
America/Boise	Asia/Hong_Kong	Europe/Tiraspol
America/Buenos_Aires	Asia/Hovd	Europe/Uzhgorod
America/Cambridge_Bay	Asia/Irkutsk	Europe/Vaduz
America/Campo_Grande	Asia/Istanbul	Europe/Vatican
America/Cancun	Asia/Jakarta	Europe/Vienna
America/Caracas	Asia/Jayapura	Europe/Vilnius
America/Catamarca	Asia/Jerusalem	Europe/Volgograd
America/Cayenne	Asia/Kabul	Europe/Warsaw
America/Cayman	Asia/Kamchatka	Europe/Zagreb
America/Chicago	Asia/Karachi	Europe/Zaporozhye
America/Chihuahua	Asia/Kashgar	Europe/Zurich
America/Coral_Harbour	Asia/Katmandu	Indian/Antananarivo
America/Cordoba	Asia/Krasnoyarsk	Indian/Chagos
America/Costa_Rica	Asia/Kuala_Lumpur	Indian/Christmas
America/Cuiaba	Asia/Kuching	Indian/Cocos
America/Curacao	Asia/Kuwait	Indian/Comoro
America/Danmarkshavn	Asia/Macao	Indian/Kerguelen
America/Dawson	Asia/Macau	Indian/Mahe
America/Dawson_Creek	Asia/Magadan	Indian/Maldives
America/Denver	Asia/Makassar	Indian/Mauritius



America/Detroit	Asia/Manila	Indian/Mayotte
America/Dominica	Asia/Muscat	Indian/Reunion
America/Edmonton	Asia/Nicosia	Mexico/BajaNorte
America/Eirunepe	Asia/Novosibirsk	Mexico/BajaSur
America/El_Salvador	Asia/Omsk	Mexico/General
America/Ensenada	Asia/Oral	Mideast/Riyadh87
America/Fort_Wayne	Asia/Phnom_Penh	Mideast/Riyadh88
America/Fortaleza	Asia/Pontianak	Mideast/Riyadh89
America/Glace_Bay	Asia/Pyongyang	Pacific/Apia
America/Godthab	Asia/Qatar	Pacific/Auckland
America/Goose_Bay	Asia/Qyzylorda	Pacific/Chatham
America/Grand_Turk	Asia/Rangoon	Pacific/Easter
America/Grenada	Asia/Riyadh	Pacific/Efate
America/Guadeloupe	Asia/Riyadh87	Pacific/Enderbury
America/Guatemala	Asia/Riyadh88	Pacific/Fakaofu
America/Guayaquil	Asia/Riyadh89	Pacific/Fiji
America/Guyana	Asia/Saigon	Pacific/Funafuti
America/Halifax	Asia/Sakhalin	Pacific/Galapagos
America/Havana	Asia/Samarkand	Pacific/Gambier
America/Hermosillo	Asia/Seoul	Pacific/Guadalcanal
America/Indiana/Indianapolis	Asia/Shanghai	Pacific/Guam
America/Indiana/Knox	Asia/Singapore	Pacific/Honolulu
America/Indiana/Marengo	Asia/Taipei	Pacific/Johnston
America/Indiana/Petersburg	Asia/Tashkent	Pacific/Kiritimati
America/Indiana/Tell_City	Asia/Tbilisi	Pacific/Kosrae
America/Indiana/Vevay	Asia/Tehran	Pacific/Kwajalein
America/Indiana/Vincennes	Asia/Tel_Aviv	Pacific/Majuro
America/Indiana/Winamac	Asia/Thimbu	Pacific/Marquesas

America/Indianapolis	Asia/Thimphu	Pacific/Midway
America/Inuvik	Asia/Tokyo	Pacific/Nauru
America/Iqaluit	Asia/Ujung_Pandang	Pacific/Niue
America/Jamaica	Asia/Ulaanbaatar	Pacific/Norfolk
America/Jujuy	Asia/Ulan_Bator	Pacific/Noumea
America/Juneau	Asia/Urumqi	Pacific/Pago_Pago
America/Kentucky/Louisville	Asia/Vientiane	Pacific/Palau
America/Kentucky/Monticello	Asia/Vladivostok	Pacific/Pitcairn
America/Knox_IN	Asia/Yakutsk	Pacific/Ponape
America/La_Paz	Asia/Yekaterinburg	Pacific/Port_Moresby
America/Lima	Asia/Yerevan	Pacific/Rarotonga
America/Los_Angeles	Atlantic/Azores	Pacific/Saipan
America/Louisville	Atlantic/Bermuda	Pacific/Samoa
America/Maceio	Atlantic/Canary	Pacific/Tahiti
America/Managua	Atlantic/Cape_Verde	Pacific/Tarawa
America/Manaus	Atlantic/Faeroe	Pacific/Tongatapu
America/Martinique	Atlantic/Faroe	Pacific/Truk
America/Mazatlan	Atlantic/Jan_Mayen	Pacific/Wake
America/Mendoza	Atlantic/Madeira	Pacific/Wallis
America/Menominee	Atlantic/Reykjavik	Pacific/Yap
America/Merida	Atlantic/South_Georgia	US/Alaska
America/Mexico_City	Atlantic/St_Helena	US/Aleutian
America/Miquelon	Atlantic/Stanley	US/Arizona
America/Moncton	Australia/ACT	US/Central
America/Monterrey	Australia/Adelaide	US/Eastern
America/Montevideo	Australia/Brisbane	US/East-Indiana
America/Montreal	Australia/Broken_Hill	US/Hawaii
America/Montserrat	Australia/Canberra	US/Indiana-Starke

---

America/Nassau	Australia/Currie	US/Michigan
America/New_York	Australia/Darwin	US/Mountain
America/Nipigon	Australia/Eucla	US/Pacific
America/Nome	Australia/Hobart	US/Pacific-New
America/Noronha	Australia/LHI	US/Samoa

## APPENDIX B      **Status Codes**

The Email Security Provisioning API returns the following status codes:

- **Error:** There is an error in the script/command that prevented its execution. Correction of the error is required before the script/command can execute successfully.
- **Warning:** There was a non-fatal error during the execution of the script/command. The error will be automatically corrected by the system within an hour.
- **Success:** The execution of the script/command was completed successfully.