

Messaging Security Suite



800-782-3762
www.edgewave.com

Red Condor is now EdgeWave

EdgeWave acquired Red Condor in 2010 to add comprehensive Messaging Security to the already existing web security solutions offering.

© 2001 - 2011 EdgeWave. All rights reserved. The EdgeWave logo is a trademark of EdgeWave 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 Messaging 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 EdgeWave.

XML08.2.0.001

Contents

Document Revisions	1
Chapter 1 API Overview	6
Chapter 2 Obtaining and Using an Authentication Token	7
Chapter 3 Configuration Download	8
Chapter 4 Configuration Upload	14
Chapter 5 XML Elements and Attributes	16
configuration.....	16
Domain Settings	16
domain.....	17
categories.....	22
category.....	22
console.....	23
digest.....	24
enemies.....	26
enemy.....	26
extensions.....	26
extension.....	26
friends.....	27
friend.....	27
languages.....	28
language.....	28
wordlists.....	29
wordlist.....	29
Outbound Settings	30
outbound.....	30
annotation.....	34
categories.....	34
category.....	34
enemies.....	35
enemy.....	35
exemptrecipients.....	35
exemptrecipient.....	35
extensions.....	36

extension	36
friends	37
friend	37
gateways	38
gateway	38
tlsdomains	38
wordlists	39
wordlist	39
Brand Settings	40
domain-defaults	41
outbound-defaults	41
Mailbox Settings	41
mailbox	41
alias	43
categories	43
category	43
console	44
digest	45
enemies	46
enemy	46
extensions	47
extension	47
friends	48
friend	48
languages	48
language	48
Language Codes	49
Chapter 6 Sample XML Code	51
Download Account List	51
Download Domain List	51
Viewing the Account Configuration	51
Adding Domains	52
Deleting Domains	53
Moving Domains between Accounts	54
Setting the User Dashboard Authentication Method	54
SMTP AUTH	54
LDAP	54
Assigning a Verifier to a Domain	55

Setting the Encryption Policy.....	55
Creating User Mailboxes.....	55
Deleting User Mailboxes.....	56
Exempting Recipients from Outbound Rate Limits.....	56
Modifying Friends and Enemies Lists.....	56
Digest Settings.....	57
Category Filter Settings.....	57
Language Filter Settings.....	58
Extension Filter Settings.....	59
Word List Filter Settings.....	59
Outbound Settings.....	60
DSN.....	60
Outbound Quarantine Access.....	61
Encryption Settings.....	61
Routing and Per-Recipient Rate Limiting.....	61
Recipient Whitelist and Authentication.....	62
Chapter 7 Command Line Scripting.....	63
Adding, Accessing and Deleting Accounts.....	63
Examples.....	64
Checking the API Version Number.....	64
Administrative User Commands.....	65
Creating a User.....	65
Assigning User Administrative Roles.....	66
Revoking User Administrative Roles.....	66
Deleting an Administrative User.....	67
Quarantine Access.....	67
Retrieving a Quarantined Messages List.....	67
Retrieving a Message.....	69
Releasing a Message.....	69
Deleting a Message.....	69
Changing a Password.....	70
Verifier Commands.....	70
Listing Verifiers.....	71
Creating a Verifier.....	71
Modifying a Verifier.....	72
Deleting a Verifier.....	73
Word List Commands.....	73
Listing Word Lists.....	74

Downloading the Contents of a Word List	75
Creating a Word List	75
Modifying a Word List	76
Deleting a Word List	76
Chapter 8 Best Practices	77
API Version Check	77
Appendix A Supported Time Zones	78
Appendix B Status Codes	87

Document Revisions

Revision	Date	Changes
10	10/10/08	<ul style="list-style-type: none">• Deprecated filtering of foreign, attachment and block_attachment. To specify foreign language delivery policy, use the language configuration element. To specify attachment delivery policy, use the extension configuration element. See Domain Settings, Mailbox Settings, Language Filter Settings, and Extension Filter Settings.• Added the ability to add and delete one or more users from the friends and enemies list. See Mailbox Settings and Modifying Friends and Enemies Lists.• You can now add account=<UID> to the config/download request URL to only return domains from a given account. This can be combined with domain=<prefix> to further restrict the list of domains. See Download Domain List.• Added the ability to download account information. See Domain Settings.
11	10/24/08	<ul style="list-style-type: none">• Added the ability to move a domain from one account to another. See Domain Settings and Moving Domains between Accounts.
12	10/31/08	<ul style="list-style-type: none">• Added command for retrieving the API version. See Checking the API Version Number.• Added new section for best practices. See Best Practices.

13	11/17/08	<ul style="list-style-type: none">• Added two commands for outbound filtering Delivery Status Notification. See Domain Settings and Outbound Settings.• Added command for enabling access to outbound filtered messages from the Personal Dashboard. See Domain Settings and Outbound Settings.
14	1/29/09	<ul style="list-style-type: none">• Added parameters for outbound filtering. See Domain Settings.• Add examples and commands for verifiers. See Setting the User Dashboard Authentication Method, Assigning a Verifier to a Domain, and Verifier Commands.
15	2/2/09	<ul style="list-style-type: none">• API version updated to 2.1.• Added Phishing as new message category. See Mailbox Settings.
16	3/31/09	<ul style="list-style-type: none">• Added domain parameters mbcleanup and maxmsgsize. See Domain Settings.• Added support for word list filtering. See Configuration Download, Domain Settings, Word List Filter Settings, and Word List Commands.
17	7/17/09	<ul style="list-style-type: none">• Added example of invalid mailbox in configuration download section. See Configuration Download and Mailbox Settings.
18	8/28/09	<ul style="list-style-type: none">• Added email parameter to Account create command. See Adding, Accessing and Deleting Accounts.
19	10/30/09	<ul style="list-style-type: none">• Added support for downloading inactive mailboxes. See Configuration Download and Mailbox Settings.

20	12/15/09	<ul style="list-style-type: none">• Added clienttls and sessiontls to domain parameters and tldsdomains as a child element to domain. See Domain Settings and tldsdomains.
21	4/14/10	<ul style="list-style-type: none">• Parameter phishing changed to phish. Phishing remains valid through this release only, then deprecated. See Domain Settings.• Parameter verified changed to VRFY. Verified remains valid through this release only, then deprecated. See Domain Settings.• Removed filter type blank.• Added filtering types credit and ssn. See categories and Mailbox Settings.• Added section about quarantine access. See Quarantine Access.• Added journaling, balanced, and spooling parameters. See Domain Settings.• Added routing and rate limiting parameters to outbound settings and examples. See Domain Settings, Domain Settings and Outbound Settings.• Added scope parameter to wordlist section. See wordlists.

22	9/2/10	<ul style="list-style-type: none"> • Changed role parameters for grant options. The older parameters are valid in for this release, but will be deprecated in future releases. See Administrative User Commands. • Domain parameter dsnlimit valid options changed from 0 to 99999 to 1 to 99999. See Domain Settings. • Added domain parameters authenticator, dhaprotection, consoleaccess, and dsnunrestricted. See Domain Settings Domain Settings and Outbound Settings. • Added exemptrecipients as child element to domain. See Domain Settings Domain Settings and Outbound Settings. • Added mailbox parameter consoleaccess. See Mailbox Settings.
23	11/2/10	<ul style="list-style-type: none"> • Added requirements for 7.3 release.
24	12/10/10	<ul style="list-style-type: none"> • Updates for Trac ticket #7752.
25	1/24/11	<ul style="list-style-type: none"> • Updates for release 7.3.1: new notifyDiscovery attribute on the domain that controls the creation of mailboxes on discovery.
26	4/28/11	<ul style="list-style-type: none"> • Added element <outbound> for outbound IP addresses. See Outbound Settings. <domain> will be deprecated for outbound IPs in a future release. • Added brand-level elements: <domain-defaults> and <outbound-defaults>. See Brand Settings. • Added categories for outbound IPs: health, finance, and profanity. See Outbound Settings. • Added category for both inbound and outbound IPs: bot. See Domain Settings Domain Settings and Outbound Settings.

27	7/26/11	<ul style="list-style-type: none">• Added emailcontinuity attribute to the <domain> element.
28	11/1/11	<ul style="list-style-type: none">• Added route attribute to the outbound <category> element.• Included Outbound IP parameters for defining Special Routing.

CHAPTER 1 **API Overview**

The Secure Messaging Provisioning API helps administrators of the Message Assurance Gateway (MAG) appliance automate configuration and maintenance of their 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>.redcondor.net` or `http://<brand>.redcondor.net`). Any information in the database not specified in the XML document is left unchanged.

The Secure Messaging 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.

CHAPTER 2 Obtaining and Using an Authentication Token

All Secure Messaging API calls require an authentication token. The return token is an opaque base64-encoded authentication token; e.g.,
YmVub2I0bUByZWRjb25kb3luY29tAAABGmV0ol-DaYnh2g9w7dVfAacwDopB1u72_g.

The token expires after 24 hours. Request a token from the dashboard with the following statement:

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

where:

Variable	Definition	Example
DASHBOARD	Host name	my.brand.redcondor.net
EMAIL	Email address	admin@domain.com
PASSWORD	Password	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:

```
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.

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=edgewave will match edgewave.com, edgewave.net, edgewaves.com.

If no domain is specified, the resulting XML document will contain the configuration for all domains in the branded dashboard.

The following is an example of a XML schema download:

```
<configuration version="2.2" timestamp="2009-04-01T22:51:47.804">
  <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.edgewave.com</Host>
        <HostListOrder>Shuffle</HostListOrder>
        <Timeout>5</Timeout>
      </LDAP>
    </Vrfy>
  </verifier>
  <domain-defaults gateway="mail.edgewave.com" clienttls="none"
  emailcontinuity="false" authenticator="" dsnunrestricted="false" maxmsgsize="5"
  spoolerduration="96" retainblocked="false" retaindelivered="true" mbcleanup="3"
  token="true" balanced="false" discovery="disabled" unrecognized="bounce" odi="true"
  notifydiscovery="true" sessionverify="false" dhaprotection="bounce_only">
    <wordlists/>
    <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">
<wordlists/>
<exemptrecipients/>
<tlsdomains policy="available"/>
<gateways/>
</outbound-defaults>
<wordlist name="Bad Words" uid="86B88D3C-F29B-6F59-6B0E-6C26603FC18B"
account="A5A659B3-6901-4D8A-B231-100C0DF2FCC0">badword01|badword02|
badword03</wordlist>
<wordlist name="Another List" uid="BFE78762-1788-4DA2-B84F-3C73D3C7EF09"
account="A5A659B3-6901-4D8A-B231-100C0DF2FCC0">badword04|badword05|
badword06</wordlist>
<domain name="example.com" notifydiscovery="true" account="C2F26595-29E2-764D-3519-
13" emailcontinuity="false" 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.edgewavearchive.com" balanced="false" spoolerduration="96">
  <digest detail="red" format="html" frequency="never" order="Date-"/>
  <categories>
    <category name="junk" action="quarantine"/>
    <category name="forged" 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"/>
  </extensions>
</domain>
```

```

    <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>
  <wordlists>
    <wordlist uid="86B88D3C-F29B-6F59-6B0E-6C26603FC18B" action="quarantine"
      scope="message"/>
    <wordlist uid="BFE78762-1788-4DA2-B84F-3C73D3C7EF09" action="quarantine"
      scope="message"/>
  </wordlists>
  <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/>
  </mailbox>
  <mailbox name="chris" status="active" consoleaccess="" timezone="" bcc="">
    <digest detail="red" format="html" frequency="daily" order="Date+"/>
    <categories>
      <category name="junk" action="quarantine"/>
    </categories>
  </mailbox>

```

```
<category name="forged" 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"/>
</extensions>
```

```

    <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"
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" 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="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>
<wordlists>
  <wordlist uid="52bd2714-a881-4772-acf2-efb82cf53bd7" action="quarantine"
    scope="message"/>
</wordlists>
<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.	true: 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. false: 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. Note: Use the true option carefully.	true: All elements in the database not specified in the XML document will be deleted. false: 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 below.



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

CHAPTER 5 XML Elements and Attributes

The following sections show the supported Messaging Security 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.	2.2
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.
outbound (read-only)	Specifies that this is an outbound IP. It only appears when an outbound IP is defined. Note: This attribute will be deprecated in a future release. See Outbound Settings for elements and attributes for outbound IPs.	true: The element is an outbound IP.
gateway	Comma separated list of the domain gateways.	Mail server.

clienttls	Encryption setting between the MAG appliance and the mail gateway.	<p>none: Encryption never offered during the session.</p> <p>available: If an encrypted session cannot be established, the message is sent in the clear.</p> <p>required: If an encrypted session can not be established then the connection is closed</p> <p>valid: The certificate must be valid.</p> <p>trusted: The certificate must be trusted.</p>
discovery	The method for discovering new mailboxes for the domain.	<p>disabled: No level of automation, you must manually enter and delete mailboxes as needed.</p> <p>verify: 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>rcpt: 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>external: Uses a previously defined verifier.</p> <p><domain_name> : 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.	true: mailbox created false: mailbox not created
unrecognized	The method for handling a message to an unknown user when the mailbox discovery is set to disabled.	accept: Forward message to customer's mail server without spam/virus filtering. bounce: Return to sender with standard 550 unrecognized recipient. discard: Deletes without sending notification. forward email address: 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 Messaging Security system.
odi	The method for handling mailbox aliases when forwarding to the mail gateway.	true: Preserves the mailbox alias before sending the message to the mail gateway. false: 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 Supported Time Zones for a list of supported time zones.
authenticator	Verifier used to validate login. Supports both inbound and outbound traffic.	UID of the custom LDAP authenticator.
authserver	Server to be used for SMTP authentication for the domain. Supports both inbound and outbound traffic.	Server IP address or host name and (optional) port number, in the format: server:portnumber
verifier	Verifier to be used for mailbox discovery.	UID of the verifier.
delete	Deletes the domain.	true: Deletes the domain.
bcc	Sends a copy of every delivered message to this Messaging Security 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. Note: Email Continuity must be licensed for this setting to have an effect.	true: Email Continuity is enabled. false: Email Continuity is disabled.
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 999
balanced	How mail is distributed when multiple mail gateways are configured.	false: Mail is sent to the first entered server. If the server is unavailable, mail goes to the second server, and so on. true: 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.	true: Allows access to outbound filtered messages through the user's Personal Dashboard. false: 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.	true: Allows access to the user's Personal Dashboard and Spam Digest. false: Disallows access to the user's Personal Dashboard and Spam Digest.

dhaprotection	Sets level of Directory Harvest Attack (DHA) protection.	<p>reject_only: All unrecognized recipients are rejected with 550 Rejected.</p> <p>reject_preference: Some unrecognized recipients are accepted for filtering and possible bounce (if not spam).</p> <p>bounce_preference: Most unrecognized recipients are accepted for filtering and possible bounce (if not spam).</p> <p>bounce_only: All unrecognized recipients are accepted for filtering and possible bounce (if not spam).</p>
retaindelivered	Attribute for keeping legitimate mail.	true or false
retainblocked	Attribute for handling blocked mail.	<p>true: Blocked mail is kept in the administrative quarantine.</p> <p>false (default): Blocked mail is deleted.</p>
token	Allows auto-login from the digest when set to true.	<p>true: User can click the link in the digest to the Personal Dashboard and be automatically logged in.</p> <p>false: Clicking the link in the digest takes the user to the Personal Dashboard, but a login is required.</p>

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, junk, forged, credit, ssn.
action	The delivery option for mail in the category. If no action is specified, the category is removed. (Required)	allow : Allows the mail to pass to the user's mailbox. markup : 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. quarantine : Sends the mail to the quarantine. block : 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 <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
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 mail from the quarantine.	true or false

digest

<digest> : Child element of <domain>.

Attribute	Description	Valid Options
-----------	-------------	---------------

<p>detail</p>	<p>Controls the (minimum) level of detail on the digest. (At least one attribute required.)</p>	<p>summary: Summary only. green: Displays only mail from the green zone (junk). yellow: Displays mail from the yellow zone (forged, foreign, attachments) plus mail from the green zone. red: Displays all mail in the quarantine.</p>
<p>format</p>	<p>Format of the daily digest. (At least one attribute required.)</p>	<p>Text, html, or multipart.</p>
<p>frequency</p>	<p>The delivery frequency of the digest. (At least one attribute required.)</p>	<p>never: The digest is not sent. daily: The digest is sent every day. weekly: The digest is sent once a week. monthly: The digest is sent once a month.</p>
<p>order</p>	<p>The order the messages in the digest are sorted. (At least one attribute required.)</p>	<p>Date-: Sorts from newest to oldest. Date+: Sorts from oldest to newest. Size-: Sorts from largest to smallest. Size+: Sorts from smallest to largest. Mailbox: Sorts on the "SMTP Mail From" field. Sender: Sorts on the "From" field in the Mime Header. Subject: Sorts by subject.</p>

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.	true : Deletes the name from the list. false : 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)	Note: 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)	allow: Allows the mail to pass to the user's mailbox. markup: 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. quarantine: Sends the mail to the quarantine. block: 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.	true: Deletes the name from the list. false: 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 Language Codes for list of supported languages.
action	Action to take on messages in selected language. If no action is specified, the language is removed. (Required)	allow: Allows the mail to pass to the user’s mailbox. markup: 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. quarantine: Sends the mail to the quarantine. block: 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.

wordlists

<wordlists> : Child element of <domain>.

wordlist

<wordlist> : Child element of <wordlists> and <domain>.

Use the <wordlist> element to add or update a specific word list. To specify the complete and authoritative set of word list-based delivery policies, enclose the <wordlist> elements in a <wordlists> element.

Attribute	Description	Valid Options
uid	UID of the word list. (Required)	GUID of a word list.
action	Action to take on the word list. If no action is specified, the word list is removed. (Required)	allow : Allows the mail to pass to the user’s mailbox. markup : 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. quarantine : Sends the mail to the quarantine. block : Deletes the mail.
markup	Text string to prepend the subject line of marked up text. (Required if action is markup.)	Text string.
scope	Which part of the message to examine. (Required)	message : Examines the whole message (default). subject : Examines the subject line only.

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 Supported Time Zones for a list of supported time zones.
authenticator	Verifier used to validate login.	UID of the custom LDAP authenticator.
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.	true : Deletes the outbound IP address.

bcc	Sends a copy of every delivered message to this Messaging 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 999.
retaindelivered	Attribute for keeping legitimate mail	true or false
sessiontls	Encryption setting between the outbound IP and the MAG appliance.	none: Encryption never offered during the session. available: If an encrypted session cannot be established, the message is sent in the clear. required: If an encrypted session can not be established then the connection is closed
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.	true : Allows notification of outbound filtered messages. false : 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.	Integer 1 through 99999 or "unlimited".

dsnunrestricted	Notification of quarantined message is sent to sender from an unknown outbound IP address.	true or false
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.	null or "" : use gateway defined by the MX records hostname : All outbound mail is sent to this server.
annotation	Enable/disable and set location of annotation in message.	None : No Annotation. prepend : The annotation will be inserted at the beginning of the message. append : 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
routeTLSPolicy	Level of encryption to use for the Special Route action.	none : Encryption is never attempted during the session. required : If an encrypted session can not be established the connection is closed. valid : The certificate must be valid. trusted : 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
 to represent
.

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, forged, credit, ssn, health, finance, profanity.
action	The delivery option for mail in the category. If no action is specified, the category is removed. (Required)	allow: Allows the mail to pass to the user’s mailbox. markup: 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. route: Sends the mail via the Special Route defined in the Outbound element.

		<p>quarantine: Sends the mail to the quarantine.</p> <p>block: 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.

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.	<p>true: Deletes the name from the list.</p> <p>false: Does not delete the name from the list.</p>

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.	true: Deletes the name from the list. false: 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)	Note: 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)	allow: Allows the mail to pass to the user's mailbox.

		<p>markup: 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>quarantine: Sends the mail to the quarantine.</p> <p>block: Deletes the mail.</p>
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.	<p>true: Deletes the name from the list.</p> <p>false: Does not delete the name from the list.</p>

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

tlsdomains

<tlsdomains> : Child element of <outbound>.

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

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

<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.	none : Encryption never attempted during the session. available : If an encrypted session cannot be established, the message is sent in the clear. required : If an encrypted session can not be established then the connection is closed valid : The certificate must be valid. trusted : 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

wordlists

<wordlists> : Child element of <outbound>.

wordlist

<wordlist> : Child element of <wordlists> and <outbound>.

Use the <wordlist> element to add or update a specific word list. To specify the complete and authoritative set of word list-based delivery policies, enclose the <wordlist> elements in a <wordlists> element.

Attribute	Description	Valid Options
uid	UID of the word list. (Required)	GUID of a word list.
action	Action to take on the word list. If no action is specified, the word list is removed. (Required)	allow : Allows the mail to pass to the user's mailbox. markup : 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. quarantine : Sends the mail to the quarantine. block : Deletes the mail.
markup	Text string to prepend the subject line of marked up text. (Required if action is markup.)	Text string.
scope	Which part of the message to examine. (Required)	message : Examines the whole message (default). subject : Examines the subject line only.

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.

mailbox

<mailbox> : Child element of <domain>.

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. 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 Supported Time Zones for a list of supported time zones.
bcc	Blind copy field of email "to" address.	Email address.
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, phishing, bot, spam, junk, forged, credit, ssn.
action	The delivery option for mail in the category. If no action is specified, the category is removed. (Required)	allow: Allows the mail to pass to the user’s mailbox. markup: 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. quarantine: Sends the mail to the quarantine. block: 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
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

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.)	summary: Summary only. green: Displays only mail from the green zone (junk). yellow: Displays mail from the yellow zone (forged, foreign, attachments) plus mail from the green zone. red: Displays all mail from the quarantine.
format	Format of the daily digest. (At least one attribute required.)	Text or html.

frequency	The frequency of the digest. If set to inherit, it uses the domain settings. (At least one attribute required.)	never : Does not send the digest. daily : Sends the digest every day. weekly : Sends the digest once a week. monthly : Sends the digest once a month.
order	The order the messages in the digest are sorted. If blank, it uses the domain settings. (At least one attribute required.)	Date- : Sorts from newest to oldest. Date+ : Sorts from oldest to newest. Size- : Sorts from largest to smallest. Size+ : Sorts from smallest to largest. Mailbox : Sorts on the "SMTP Mail From" field. Sender : Sorts on the "From" field in the Mime Header. Subject : 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.	true: Deletes the name from the list. false: 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)	Note: 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)	allow: Allows the mail to pass to the user's mailbox. markup: 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. quarantine: Sends the mail to the quarantine. block: 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.	true : Deletes the name from the list. false : Does not delete the name from the list.

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 Language Codes for list of supported languages.
action	Action to take on messages in selected language. If no action is specified, the language is removed.	allow : Allows the mail to pass to the user’s mailbox. markup : 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. quarantine : Sends the mail to the quarantine. block : 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.

Language Codes

The table below shows the languages supported in the Messaging 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 Messaging 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". This ensures that the URL is valid and spaces should be encoded 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 to a subset of that, 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.redcondor.net"/>
</result>
```

Adding Domains

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-CAFD246F47"
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"/>
    <category name="forged" 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"/>
  </languages>
</configuration>
```

```
<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>
<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"/>
  <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 Domains

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

```
<domain name="example.com" account="C653622B-22A1-21BB-CD7F-CAFD246F47"
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. Messaging Security supports:

- **Internal:** ID and password are stored on the EdgeWave Messaging 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 MAG to the mail gateway:

```
<domain name="example.comt" 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 address to the friends and enemies list of the "aaron" mailbox, and an alias to the "adserl" mailbox. The "adrian" mailbox has no Personal Dashboard access.

```
<domain name="example.com">
  <mailbox name="aaron">
    <friend name="temp@edgewave.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>
```

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>
```

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="forged" action="markup" markup="FORGED?"/>
    <category name="virus" action="markup" markup="VIRUS:"/>
    <category name="adult" action="markup" markup="ADLT:"/>
    <category name="phish" action="quarantine"/>
    <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.

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"/>
    <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>
```

```
</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.

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.

Word List Filter Settings

The following example adds a word list filter for the domain example.com that examines the whole message and quarantines the filtered mail:

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

```
</domain>
```

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

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

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

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

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

```
<domain name="example.com">
  <wordlists>
    <wordlist uid="86B88D3C-F29B-6F59-6B0E-6C26603FC18B" action="quarantine"
      scope="subject"/>
    <wordlist uid="BFE78762-1788-4DA2-B84F-3C73D3C7EF09" action="quarantine"
      scope="message"/>
  </wordlists>
</domain>
```

The following example updates a word list filter to markup a message for the domain example.com. The scope attribute is not included, so it is not updated.

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

Outbound Settings

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 MAG appliance. The default encryption policy between the MAG appliance 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=""signature+/>
  </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, 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!"
sessionstls="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 Messaging 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.

Adding, Accessing and Deleting Accounts

Option	Parameter	Description	Valid Options
list	<none>	Returns a list of all accounts	NA
list	name	Returns a list of all accounts starting with the text assigned to name	Any text string

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 timezone	
delete		Delete the account with the given ID	
	account	The account to delete	UID for the account

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://my.test.redcondor.net/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"
```

Checking the API Version Number

The following command retrieves the Messaging Security API version number:

```
curl "http://$brand/api/version"
```

Sample output:

2.2.

Administrative User Commands

Option	Parameter	Description	Valid Options
create		Adds a user to the system with the given ID and password.	
	email	User ID.	Valid email address.
	password	User password.	Minimum 6 alphanumeric characters.
delete		Delete the user with the given ID.	
	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.	sa: system administrator account: account administrator domain: account operator operator: dashboard operator

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.

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=aa"
```

Where "\$ACCOUNT" is the UID of the account. See [Configuration Download](#) for more information about UIDs. 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.

Supported roles are:

- **sa:** system administrator
- **aa:** account administrator
- **ao:** account operator
- **do:** dashboard operator

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"
```

Where "\$ACCOUNT" is the UID of the account. If the account is not specified, all permissions for the user are revoked from all accounts. You cannot revoke permissions for the user of the API.

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

The token used in the commands below 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](#).

Retrieving a Quarantined Messages List

To acquire a list of quarantined messages for a given user and date range, issue the following command:

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

Messages received between the <from> date and the <to> date are returned in the list. The dates must be in GMT and in the following format: (yyyy-MM-ddTHH:mm:ss.SSS). For example: 2010-04-21T13:46:01.345.

The date range is optional. If <from> is not specified, the list starts with the oldest message. If <to> is not specified, the list ends with the most recent message.



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

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

For each message, the following attributes are returned:

- **id**: this is an opaque id for the message used to view, delete and release the message received: the 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 http://www.iso.org/iso/english_country_names_and_code_elements
- **category**: can be any of the filtering categories supported by the application. For example, junk, forged, foreign, attachment, keyword, enemy, friend, virus, phish, bot, adult, ssn, credit, or spam
- **zone**: green, yellow or red based on the category
- **reason**: an internal field identifying the responsible spam filter rule

Retrieving a Message

To retrieve a specific message, enter the following command:

```
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, enter the following command:

```
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://svt3.edgewave.net/api/quarantine/release?token=$TOKEN&id=20100415235914550@8f223846-d126-4ea4-8563-457fdd82d38f"
```

Release multiple messages with one command using the following command:

```
curl "http://$DASHBOARD/api/quarantine/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>"
```

Where <id> is the message identifier.

For example:

```
curl "http://svt3.edgewave.net/api/quarantine/delete?token=$TOKEN&id=20100416183935248@8f223846-d126-4ea4-8563-457fdd82d38f"
```

To delete multiple messages with one command:

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

Where <idx> is the message identifier "id".

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).

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
list		Returns a list of all verifiers.	NA
list	account	Returns a list of all verifiers in an account.	Account UID
list	UID	Returns the verifier contents in XML format.	Valid UID
list	UID	Returns the verifier contents in plain text format.	Valid UID
	plain	Flag indicating the list format.	true
create		Adds a verifier to the system.	
	name	Name of the Verifier.	Any text string
	account	Creates a verifier for a specific account.	UID of the account. Empty makes it a system-wide verifier.
	xml	XML verifier definition.	Definition coming soon

update		Modifies a verifier.	
	UID	UID of the verifier to update.	Valid UID
	account	Reassigns the verifier to a specific account. Optional.	UID of the account
	xml	XML verifier definition.	
delete		Deletes a verifier.	
	UID	UID of the verifier to delete.	

Listing Verifiers

To download a list of all verifiers in a brand (for example, xxx.edgewave.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:

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

Modifying a Verifier

You can modify the name, XML definition, or reassign the verifier to a different account. 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 name of the verifier to test:

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

Where `xxxxxxx` is the UID of the verifier and `"test"` is the new name of the verifier.

The following example assigns the verifier to `$ACCOUNT`:

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

Where `xxxxxxx` is the UID of the verifier; and `"$ACCOUNT"` is the UID of the new account to assign it to.

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

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

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

The following example combines all three examples from above into one command. The verifier name is updated, it is assigned to a different account, and the verifier definition is modified.

```
curl
"http://$DASHBOARD/api/verifier/update?token=$TOKEN&uid=xxxxxxx&name=test&account=$ACCOUNT&xm
```

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=$vrfy_uid&account=$account_uid"
```

Deleting a Verifier

To delete a verifier, enter the following:

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

Where xxxxxx is the UID of the verifier.

Word List Commands

Word lists are used in keyword filtering to detect messages containing specific words in the subject line, 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 word lists in an account, then activate lists on individual domains as needed.

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

Create a word list in an account for keyword filtering. Create as many individual lists as needed, then assign one or more word lists to individual domains or outbound IPs as appropriate.

You can enter the keywords, phrases, and regular expressions individually or copy the word list from a text editor or word processor and paste it into the screen. 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
list		Returns a list of all word lists.	NA

list	account	Returns a list of all word lists in an account.	Account UID.
list	UID	Returns the word list contents in XML format	Valid UID.
list	UID	Returns the word list contents in plain text format.	Valid UID.
	plain	Flag indicating list format.	true
create		Adds a word list to the system.	
	name	Name of the word list.	Any text string
	account	Creates a word list for a specific account.	UID of the account. Empty makes it a system-wide word list.
update		Modifies a word list.	
	UID	UID of the word list to update.	Valid UID
	account	Adds and removes words from a word list.	UID of the account.
delete		Deletes a word list.	
	UID	UID of the word list to delete.	

Listing Word Lists

To download a list of all word lists in a brand (for example, xxx.edgewave.net) with complete details, enter the following statement:

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

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

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

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

Downloading the Contents of a Word List

The following command downloads all of the word lists for the brand:

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

The following command downloads all the word lists for the given account UID:

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

The following command downloads the contents of the word list for the given word list UID in XML format:

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

The following command downloads the plain text contents of the word list for the given word list UID:

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

Creating a Word List

Separate individual words in a word list with a pipe (|). You can use A-Z, a-z, 0-9, hyphen(-), or underscore(_) to match words. Keywords are not case sensitive.

To create a word list using a datafile, enter the following statement:

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

Where "wordlist.txt" is the datafile containing the list of words separated by a | (pipe) or carriage return.

To create a word list by streaming words, enter the following statement:

```
echo "badword01|badword02|badword03" | curl -H 'Content-type: text/plain' --data-binary @- "$DASHBOARD/api/wordlist/create?token=$TOKEN&name=test&account=$ACCOUNT"
```

Where "badword01|badword02|badword03" is the list of words.

Modifying a Word List

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

The following example reads from the text file `worldlist01.txt` and replaces the word list identified by the given UID with the contents of the file:

```
curl -F "data=@wordlists/worldlist01.txt"
"http://$DASHBOARD/api/wordlist/update?uid=FFF1DAFF-8BBC-4C17-953B-
287423F52312&token=$TOKEN"
```

The following example changes the name of the word list specified with the token to `worldlist02`:

```
curl "http://$DASHBOARD/api/wordlist/update?&token=$TOKEN&uid=FC9DBB74-16D9-4CA1-
9704-DF62D744705&name=worldlist02"
```

The following example updates the word list by replacing the contents of the list with the words `badword01`, `badword02`, and `badword03`:

```
echo "badword01|badword02|badword03" | curl -H 'Content-type: text/plain' --data-
binary @- "$DASHBOARD/api/wordlist/update?token=$TOKEN&account=A5A659B3-6901-4D8A-
B231-100C0DF2FCC0&uid=47A0E318-1AA2-4F54-B825-D3464C74288E"
```

Deleting a Word List

To delete a word list:

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

CHAPTER 8 **Best Practices**

This section contains the best practices for using the Secure Messaging API in real-world deployments.

API Version Check

The Secure Messaging 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.

EdgeWave strongly recommends that when using the API, you issue a version check as the first part of the script. If the version does not match, the script should error out. See [Checking the API Version Number](#) for more information.

APPENDIX A Supported Time Zones

The table below shows the supported time zones:

Africa/Abidjan	America/Resolute	Etc/GMT+0
Africa/Accra	America/Rio_Branco	Etc/GMT+1
Africa/Addis_Ababa	America/Rosario	Etc/GMT+10
Africa/Algiers	America/Santiago	Etc/GMT+11
Africa/Asmara	America/Santo_Domingo	Etc/GMT+12
Africa/Asmera	America/Sao_Paulo	Etc/GMT+2
Africa/Bamako	America/Scoresbysund	Etc/GMT+3
Africa/Bangui	America/Shiprock	Etc/GMT+4
Africa/Banjul	America/St_Johns	Etc/GMT+5
Africa/Bissau	America/St_Kitts	Etc/GMT+6
Africa/Blantyre	America/St_Lucia	Etc/GMT+7
Africa/Brazzaville	America/St_Thomas	Etc/GMT+8
Africa/Bujumbura	America/St_Vincent	Etc/GMT+9
Africa/Cairo	America/Swift_Current	Etc/GMT0
Africa/Casablanca	America/Tegucigalpa	Etc/GMT-0

Africa/Ceuta	America/Thule	Etc/GMT-1
Africa/Conakry	America/Thunder_Bay	Etc/GMT-10
Africa/Dakar	America/Tijuana	Etc/GMT-11
Africa/Dar_es_Salaam	America/Toronto	Etc/GMT-12
Africa/Djibouti	America/Tortola	Etc/GMT-13
Africa/Douala	America/Vancouver	Etc/GMT-14
Africa/El_Aaiun	America/Virgin	Etc/GMT-2
Africa/Freetown	America/Whitehorse	Etc/GMT-3
Africa/Gaborone	America/Winnipeg	Etc/GMT-4
Africa/Harare	America/Yakutat	Etc/GMT-5
Africa/Johannesburg	America/Yellowknife	Etc/GMT-6
Africa/Kampala	Antarctica/Casey	Etc/GMT-7
Africa/Khartoum	Antarctica/Davis	Etc/GMT-8
Africa/Kigali	Antarctica/DumontDUrville	Etc/GMT-9
Africa/Kinshasa	Antarctica/Mawson	Etc/Greenwich
Africa/Lagos	Antarctica/McMurdo	Etc/UCT
Africa/Libreville	Antarctica/Palmer	Etc/Universal
Africa/Lome	Antarctica/Rothera	Etc/UTC
Africa/Luanda	Antarctica/South_Pole	Etc/Zulu
Africa/Lubumbashi	Antarctica/Syowa	Europe/Amsterdam
Africa/Lusaka	Antarctica/Vostok	Europe/Andorra

Africa/Malabo	Arctic/Longyearbyen	Europe/Athens
Africa/Maputo	Asia/Aden	Europe/Belfast
Africa/Maseru	Asia/Almaty	Europe/Belgrade
Africa/Mbabane	Asia/Amman	Europe/Berlin
Africa/Mogadishu	Asia/Anadyr	Europe/Bratislava
Africa/Monrovia	Asia/Aqtau	Europe/Brussels
Africa/Nairobi	Asia/Aqtobe	Europe/Bucharest
Africa/Ndjamena	Asia/Ashgabat	Europe/Budapest
Africa/Niamey	Asia/Ashkhabad	Europe/Chisinau
Africa/Nouakchott	Asia/Baghdad	Europe/Copenhagen
Africa/Ouagadougou	Asia/Bahrain	Europe/Dublin
Africa/Porto-Novo	Asia/Baku	Europe/Gibraltar
Africa/Sao_Tome	Asia/Bangkok	Europe/Guernsey
Africa/Timbuktu	Asia/Beirut	Europe/Helsinki
Africa/Tripoli	Asia/Bishkek	Europe/Isle_of_Man
Africa/Tunis	Asia/Brunei	Europe/Istanbul
Africa/Windhoek	Asia/Calcutta	Europe/Jersey
America/Adak	Asia/Choibalsan	Europe/Kaliningrad
America/Anchorage	Asia/Chongqing	Europe/Kiev
America/Anguilla	Asia/Chungking	Europe/Lisbon
America/Antigua	Asia/Colombo	Europe/Ljubljana

America/Araguaina	Asia/Dacca	Europe/London
America/Argentina/Buenos_Aires	Asia/Damascus	Europe/Luxembourg
America/Argentina/Catamarca	Asia/Dhaka	Europe/Madrid
America/Argentina/ComodRivadavia	Asia/Dili	Europe/Malta
America/Argentina/Cordoba	Asia/Dubai	Europe/Mariehamn
America/Argentina/Jujuy	Asia/Dushanbe	Europe/Minsk
America/Argentina/La_Rioja	Asia/Gaza	Europe/Monaco
America/Argentina/Mendoza	Asia/Harbin	Europe/Moscow
America/Argentina/Rio_Gallegos	Asia/Hong_Kong	Europe/Nicosia
America/Argentina/San_Juan	Asia/Hovd	Europe/Oslo
America/Argentina/Tucuman	Asia/Irkutsk	Europe/Paris
America/Argentina/Ushuaia	Asia/Istanbul	Europe/Podgorica
America/Aruba	Asia/Jakarta	Europe/Prague
America/Asuncion	Asia/Jayapura	Europe/Riga
America/Atikokan	Asia/Jerusalem	Europe/Rome
America/Atka	Asia/Kabul	Europe/Samara
America/Bahia	Asia/Kamchatka	Europe/San_Marino
America/Barbados	Asia/Karachi	Europe/Sarajevo
America/Belem	Asia/Kashgar	Europe/Simferopol
America/Belize	Asia/Katmandu	Europe/Skopje
America/Blanc-Sablon	Asia/Krasnoyarsk	Europe/Sofia

America/Boa_Vista	Asia/Kuala_Lumpur	Europe/Stockholm
America/Bogota	Asia/Kuching	Europe/Tallinn
America/Boise	Asia/Kuwait	Europe/Tirane
America/Buenos_Aires	Asia/Macao	Europe/Tiraspol
America/Cambridge_Bay	Asia/Macau	Europe/Uzhgorod
America/Campo_Grande	Asia/Magadan	Europe/Vaduz
America/Cancun	Asia/Makassar	Europe/Vatican
America/Caracas	Asia/Manila	Europe/Vienna
America/Catamarca	Asia/Muscat	Europe/Vilnius
America/Cayenne	Asia/Nicosia	Europe/Volgograd
America/Cayman	Asia/Novosibirsk	Europe/Warsaw
America/Chicago	Asia/Omsk	Europe/Zagreb
America/Chihuahua	Asia/Oral	Europe/Zaporozhye
America/Coral_Harbour	Asia/Phnom_Penh	Europe/Zurich
America/Cordoba	Asia/Pontianak	Indian/Antananarivo
America/Costa_Rica	Asia/Pyongyang	Indian/Chagos
America/Cuiaba	Asia/Qatar	Indian/Christmas
America/Curacao	Asia/Qyzylorda	Indian/Cocos
America/Danmarkshavn	Asia/Rangoon	Indian/Comoro
America/Dawson	Asia/Riyadh	Indian/Kerguelen
America/Dawson_Creek	Asia/Riyadh87	Indian/Mahe

America/Denver	Asia/Riyadh88	Indian/Maldives
America/Detroit	Asia/Riyadh89	Indian/Mauritius
America/Dominica	Asia/Saigon	Indian/Mayotte
America/Edmonton	Asia/Sakhalin	Indian/Reunion
America/Eirunepe	Asia/Samarkand	Mexico/BajaNorte
America/El_Salvador	Asia/Seoul	Mexico/BajaSur
America/Ensenada	Asia/Shanghai	Mexico/General
America/Fort_Wayne	Asia/Singapore	Mideast/Riyadh87
America/Fortaleza	Asia/Taipei	Mideast/Riyadh88
America/Glace_Bay	Asia/Tashkent	Mideast/Riyadh89
America/Godthab	Asia/Tbilisi	Pacific/Apia
America/Goose_Bay	Asia/Tehran	Pacific/Auckland
America/Grand_Turk	Asia/Tel_Aviv	Pacific/Chatham
America/Grenada	Asia/Thimbu	Pacific/Easter
America/Guadeloupe	Asia/Thimphu	Pacific/Efate
America/Guatemala	Asia/Tokyo	Pacific/Enderbury
America/Guayaquil	Asia/Ujung_Pandang	Pacific/Fakaofu
America/Guyana	Asia/Ulaanbaatar	Pacific/Fiji
America/Halifax	Asia/Ulan_Bator	Pacific/Funafuti
America/Havana	Asia/Urumqi	Pacific/Galapagos
America/Hermosillo	Asia/Vientiane	Pacific/Gambier

America/Indiana/Indianapolis	Asia/Vladivostok	Pacific/Guadalcanal
America/Indiana/Knox	Asia/Yakutsk	Pacific/Guam
America/Indiana/Marengo	Asia/Yekaterinburg	Pacific/Honolulu
America/Indiana/Petersburg	Asia/Yerevan	Pacific/Johnston
America/Indiana/Tell_City	Atlantic/Azores	Pacific/Kiritimati
America/Indiana/Vevay	Atlantic/Bermuda	Pacific/Kosrae
America/Indiana/Vincennes	Atlantic/Canary	Pacific/Kwajalein
America/Indiana/Winamac	Atlantic/Cape_Verde	Pacific/Majuro
America/Indianapolis	Atlantic/Faeroe	Pacific/Marquesas
America/Inuvik	Atlantic/Faroe	Pacific/Midway
America/Iqaluit	Atlantic/Jan_Mayen	Pacific/Nauru
America/Jamaica	Atlantic/Madeira	Pacific/Niue
America/Jujuy	Atlantic/Reykjavik	Pacific/Norfolk
America/Juneau	Atlantic/South_Georgia	Pacific/Noumea
America/Kentucky/Louisville	Atlantic/St_Helena	Pacific/Pago_Pago
America/Kentucky/Monticello	Atlantic/Stanley	Pacific/Palau
America/Knox_IN	Australia/ACT	Pacific/Pitcairn
America/La_Paz	Australia/Adelaide	Pacific/Ponape
America/Lima	Australia/Brisbane	Pacific/Port_Moresby
America/Los_Angeles	Australia/Broken_Hill	Pacific/Rarotonga
America/Louisville	Australia/Canberra	Pacific/Saipan

America/Maceio	Australia/Currie	Pacific/Samoa
America/Managua	Australia/Darwin	Pacific/Tahiti
America/Manaus	Australia/Eucla	Pacific/Tarawa
America/Martinique	Australia/Hobart	Pacific/Tongatapu
America/Mazatlan	Australia/LHI	Pacific/Truk
America/Mendoza	Australia/Lindeman	Pacific/Wake
America/Menominee	Australia/Lord_Howe	Pacific/Wallis
America/Merida	Australia/Melbourne	Pacific/Yap
America/Mexico_City	Australia/North	SystemV/AST4
America/Miquelon	Australia/NSW	SystemV/AST4ADT
America/Moncton	Australia/Perth	SystemV/CST6
America/Monterrey	Australia/Queensland	SystemV/CST6CDT
America/Montevideo	Australia/South	SystemV/EST5
America/Montreal	Australia/Sydney	SystemV/EST5EDT
America/Montserrat	Australia/Tasmania	SystemV/HST10
America/Nassau	Australia/Victoria	SystemV/MST7
America/New_York	Australia/West	SystemV/MST7MDT
America/Nipigon	Australia/Yancowinna	SystemV/PST8
America/Nome	Brazil/Acre	SystemV/PST8PDT
America/Noronha	Brazil/DeNoronha	SystemV/YST9
America/North_Dakota/Center	Brazil/East	SystemV/YST9YDT

America/North_Dakota/New_Salem	Brazil/West	US/Alaska
America/Panama	Canada/Atlantic	US/Aleutian
America/Pangnirtung	Canada/Central	US/Arizona
America/Paramaribo	Canada/Eastern	US/Central
America/Phoenix	Canada/East-Saskatchewan	US/Eastern
America/Port_of_Spain	Canada/Mountain	US/East-Indiana
America/Port-au-Prince	Canada/Newfoundland	US/Hawaii
America/Porto_Acre	Canada/Pacific	US/Indiana-Starke
America/Porto_Velho	Canada/Saskatchewan	US/Michigan
America/Puerto_Rico	Canada/Yukon	US/Mountain
America/Rainy_River	Chile/Continental	US/Pacific
America/Rankin_Inlet	Chile/EasterIsland	US/Pacific-New
America/Recife	Etc/GMT	US/Samoa
America/Regina		

APPENDIX B **Status Codes**

The Messaging 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.



Corporate Office

15333 Avenue of Science, San Diego, CA 92128

Phone: 858-676-2277

Toll Free: 800-782-3762

Fax: 858-676-2299

Email: info@edgewave.com