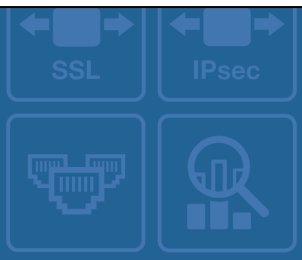
FORTINET

High Performance Network Security

FortiMail™ REST API Reference

Version 5.4



FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

FORTINET COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdocs@fortinet.com

September 13, 2017

TABLE OF CONTENTS

Introduction

This document provides the REST API information supported in FortiMail version 5.3.4 release. This document covers the FortiMail GUI supported REST API reference only. These APIs can be used to retrieve, create, update and delete configuration settings, to retrieve dynamic system statistics, and to perform basic administrative actions such as reboot and shut down.

When using the APIs, the following conventions are followed:

`Http GET` --- To retrieve all resources or particular resource

`Http POST` --- To create a new resource or perform certain administrative actions

`Http PUT` --- To update an existing resource

`Http Delete` --- To delete an existing resource

Enabling REST API support

By default, this feature is disabled on FortiMail. To enable it, use the following CLI command:

```
config system global
      set rest-api enable
end
```

Authentication

When making requests to FortiMail appliance using the REST API, you will need to pass the authentication. There are two authentication options you can use:

- PKI certificate-based authentication
- Local user password-based authentication

You also need the appropriate admin profile to access the FortiMail resources.

PKI authentication

For PKI certificate-based authentication, you must create two certificates using the same CA. One certificate will be used for FML HTTP server and the other certificate will be associated with an admin user. Both the user certificates and private key has to be moved to the PC running the script. The CA certificate needs to be copied to the PC as well. Otherwise CURL will not be able to verify the FML certificate.

To use PKI admin authentication

1. Enable PKI mode with the following CLI command:

```
config system global
      set pki-mode enable
end
```

2. Create a PKI user under *User > PKI User*.
3. Create an admin account using PKI authentication type under *System > Administrator*.
4. Split the PKCS12 certificate into cert and key. They will be used when you log in to FortiMail.

```
openssl pkcs12 -in test.p12 -out test.pem -nokeys
openssl pkcs12 -in test.p12 -out test.key nocerts -nodes
```

Password-based authentication

To establish a valid authentication session, you must make a POST request to the FortiMail login handler with your admin username and password. The POST request should contain JSON data with 'name' and 'password' fields:

URL: `http(s)://host_or_ip/api/v1/AdminLogin/`

Method: `POST`

JSON: `{"name": "admin", "password": "****"}`

If login is successful, the response will contain the authentication token in the APSCOOKIE cookie value. This cookie value must be included in any further requests.

Note: The permissions for the administrative account you use will affect which objects and operations you'll have access to, so ensure the user has the permissions required for the actions you wish to perform.

FortiMail REST API HTTP response codes

FortiMail REST APIs use well-defined HTTP status codes to indicate query results to the API. Following are some of the HTTP status codes used:

HTTP Response Code	Description

200-OK	API request successful.
400- Bad Request	Bad request.
403 - Forbidden	Request is missing authentication token or administrator is missing access profile permissions.
404- Not Found	Unable to find the specified resource.
405- Method Not Allowed	Specified HTTP method is not allowed for this resource
500	Internal Server Error

REST API for system level resources

FortiMail supports retrieval and modification of system level CMDB configuration settings as well as system level statistics. The API can be accessed using the following URL:

http(s)://host_ip/api/v1/resource_name/resource_id/sub_resource_name/sub_resource_id/

where:

`resource_name` --- Specifies the type of resource to query (such as SysInterface), required.

`resource_id` --- Unique ID of the resource as specified by resource_name (such as port1), optional. If not present, returns entire list of resources.

`sub_resource_name` --- Some resources may have sub / child resources, use this to query sub resources, optional

`sub_resource_id` --- Unique ID of the sub resource as specified by sub_resource_name, optional. If not present, returns entire list of sub resources.

Examples:

`…/api/v1/SysInterface/` --- returns list of network interfaces

`…/api/v1/SysInterface/port1/` --- return details of network interface 'port1'

`…/api/v1/SysGlobal/` --- returns details of global settings (only one instance)

`…/api/v1/ProfSession/inbound/ ProfSessionSenderWhitelist/`

--- returns sender whitelist/saftlist of session profile 'inbound'

For a full list of system level resources, refer to the Supported Resources List.

REST API for domain level resources

FortiMail also supports retrieval and modification of domain level CMDB configuration settings. The API can be accessed using the following URL:

```
http(s)://host_ip/api/v1/domain/domain_name/resource_name/resource_id/sub_resource_name/sub_resource_id/
```

It is very similar to the URL for system level resources, only two new tokens are added:

`domain` --- Required keyword, use to perform domain level queries

`domain_name` --- FQDN name of the domain to query (such as fortinet.com)

Examples:

`…/api/v1/domain/abc.com/ProfAntispam/`

--- returns list of antispam profiles for domain 'abc.com'

`…/api/v1/domain/abc.com/PolicyRcpt/`

--- returns list of recipient based policies for domain 'abc.com'

`…/api/v1/domain/abc.com/PolicyRecipient/1/`

--- returns details of recipient based policy '1' for domain 'abc.com'

For a full list of domain level resources, refer to the Supported Resources List.

REST API for administrative actions

Apart from resources, FortiMail REST API supports basic administrative actions such as restarting / shutting down a device. Use the following URL to send action request:

URL: `http(s)://host_ip/api/v1/SysStatusCommand/`

Method: `POST`

JSON: `{"action": action_value}`

Where action_value is one of the following integers:

1 --- Restart

2 --- Shut down

3 --- Reload

System resource list and URLs

Note: Resources marked with * also apply to domain level REST APIs.

URL	HTTP Method	Summary
/Addressbook/ *	GET, POST, PUT, DELETE	Contacts
/AddressbookGroup/ *	GET, POST, PUT, DELETE	Contact groups
/ArchAccount/	GET, POST, PUT, DELETE	Archive accounts
/ArchExempt/	GET, POST, PUT, DELETE	Archive exempt policy
/ArchJournalSource/	GET, POST, PUT, DELETE	Archive journaling source
/ArchPolicy/	GET, POST, PUT, DELETE	Archive policy
/AsBounceverifyKey/	GET, POST, PUT, DELETE	Bounce verification keys
/AsDeepheader/	GET, PUT	Deep header analysis settings
/AsGreylist/	GET	Greylist
/AsGreylisyAutoexempt/	GET	Auto exempt greylist
/AsMsisdnReputationAuto_blacklist/	GET	Endpoint reputation auto blocklist
/AsMsisdnReputationBlacklist/	GET, DELETE	Endpoint reputation blocklist
/AsMsisdnReputationExempt/	GET, DELETE	Endoint reputation exempt list
/AsSenderReputation/	GET	Sender reputation list
/AsSpamreport/	GET, PUT	Quarantine / spam report

		settings
/AsUrl_fgas_exempt_list/	GET, POST, PUT, DELETE	URL exempt list
/CalResource/ *	GET, POST, PUT, DELETE	
/CalendarServer/	GET, PUT	Calendar server settings
/CentralBackupConfig/	GET, PUT	Central backup configuration
/CentralConfigList/	GET, DELETE	Central backup list
/ContentScanRules/	GET, POST, PUT, DELETE	DLP content scan rules
/ContentScanRulesConditions/	GET, POST, PUT, DELETE	DLP content scan rule conditions
/ContentScanRulesExceptions/	GET, POST, PUT, DELETE	DLP content scan rule exceptions
/domain/	GET, POST, PUT, DELETE	Protected domain settings
/DomainSettingSenderAddrRateCtrlExempt/	GET, POST, PUT, DELETE	Sender rate control exempt list for specified domain settings
/DomainSpamReportRcpt/	GET, PUT	Domain level quarantine / spam report settings
/FilePattern/ *	GET, POST, PUT, DELETE	File patterns / filters
/FileSignature/	GET, POST, PUT, DELETE	File signatures for AV scan
/Fingerprint_doc/	GET, DELETE	Fingerprint document list
/LogAltMMailto/	GET, POST, DELETE	Alert email accounts
/LogAltMSetting/	GET, PUT	Alert email settings
/LogReport_config/	GET, POST, PUT,	Log report configurations

	DELETE	
/LogReportFile/	GET, DELETE	Log report files
/LogSetLocal/	GET, PUT	Local log settings
/MailSetStrgNfs/	GET, PUT	Mail storage settings
/MailSetStrgRemote_storage_ibe/	GET, PUT	Centralized IBE storage settings
/MailSetStrgServer/	GET, PUT	Centralized quarantine storage settings
/MailSetSystemquarantine/	GET, PUT	System quarantine settings
/MailSetSystemquarantineFolder/	GET, POST, PUT, DELETE	System quarantine folders
/PolicyIp/	GET, POST, PUT, DELETE	IP policies
/PolicyRecipient/ *	GET, POST, PUT, DELETE	Recipient policies
/ProfAntispam/ *	GET, POST, PUT, DELETE	AntiSpam profiles
/ProfAntispam_action/ *	GET, POST, PUT, DELETE	AntiSpam action profiles
/ProfAntispamBannedwords/ *	GET, POST, PUT, DELETE	AntiSpam profile banned words
/ProfAntispamDnsblServer/ *	GET, POST, PUT, DELETE	AntiSpam profile DNSBL servers
/ProfAntispamSurblServer/ *	GET, POST, PUT, DELETE	AntiSpam profile SURBL servers
/ProfAntispamWhitelistwords/ *	GET, POST, PUT, DELETE	AntiSpam profile safelist words
/ProfAntivirus/ *	GET, POST, PUT, DELETE	AntiVirus profiles
/ProfAntivirus_action/	GET, POST, PUT,	AntiVirus action profiles

*	DELETE	
/ProfAuthImap/ *	GET, POST, PUT, DELETE	IMAP authentication profiles
/ProfAuthPop3/ *	GET, POST, PUT, DELETE	POP3 authentication profiles
/ProfAuthRadius/ *	GET, POST, PUT, DELETE	Radius authentication profiles
/ProfAuthSmtp/ *	GET, POST, PUT, DELETE	Smtp authentication profiles
/ProfCertificate_binding/	GET, POST, PUT, DELETE	Certificate binding profiles
/ProfContent/ *	GET, POST, PUT, DELETE	Content profiles
/ProfContent_action/ *	GET, POST, PUT, DELETE	Content action profiles
/ProfContentAttachment/ *	GET, POST, PUT, DELETE	Content profile attachment scan rules
/ProfContentMonitor/ *	GET, POST, PUT, DELETE	Content monitor profile
/ProfDictionary/	GET, POST, PUT, DELETE	Dictionary profiles
/ProfDictionary_group/	GET, POST, PUT, DELETE	Dictionary group
/ProfDictionaryDictionaryItem/	GET, POST, PUT, DELETE	Dictionary profile dictionary entries
/ProfDlp/	GET, POST, PUT, DELETE	DLP profiles
/ProfDlpContentScan/	GET, POST, PUT, DELETE	DLP profile content scan settings
/ProfEmail_address_group/	GET, POST, PUT, DELETE	Email address groups

/ProfEncryption/	GET, POST, PUT, DELETE	Encryption profiles
/ProfIp_address_group/	GET, POST, PUT, DELETE	IP address groups
/ProfIp_pool/	GET, POST, PUT, DELETE	IP pools
/ProfLdap/	GET, POST, PUT, DELETE	LDAP profiles
/ProfMisc/ *	GET, POST, PUT, DELETE	Resource profiles
/ProfNotification/	GET, POST, PUT, DELETE	Notification profiles
/ProfSessionRecipientWhitelist/	GET, POST, PUT, DELETE	Session profile recipient safelist
/ProfSessionRemovedHeader/	GET, POST, PUT, DELETE	Session profile removed headers
/ProfSessionSenderBlacklist/	GET, POST, PUT, DELETE	Session profile sender blocklist
/ProfSessionSenderWhitelist/	GET, POST, PUT, DELETE	Session profile sender safelist
/ProfTls/	GET, POST, PUT, DELETE	TLS profiles
/ProfUri_filter/	GET, POST, PUT, DELETE	URI filter profiles
/RaidSystem/	GET	Raid system status
/RaidSystemArray/	GET	Raid array information
/RaidSystemDisk/	GET	Raid disk information
/SemailDbDomain/	GET, DELETE	IBE domains
/SemailDbUser/	GET, DELETE	IBE users
/Sensitive_dataCompliance/	GET	DLP standard compliance

		data
/Sensitive_dataFingerprint/	GET, POST, PUT, DELETE	DLP fingerprint data
/Sensitive_dataFingerprint_source/	GET, POST, PUT, DELETE	DLP fingerprint source
/Sensitive_dataFingerprintDocument/	GET, DELETE	DLP fingerprint documents
/SysAccprofile/	GET, POST, PUT, DELETE	Admin access profiles
/SysAdmin/	GET, POST, PUT, DELETE	System administrators
/SysAntispam/	GET, PUT	System AntiSpam settings
/SysAppearance/	GET, PUT	System appearance settings
/SysAutoupdate/	GET, PUT	FortiGuard AntiVirus auto update settings
/SysBackup_restore/	GET, PUT	Mail data auto backup settings
/SysBurstRestore/	PUT	Restore mail data from backup
/SysDateSetting/	GET, PUT	System date
/SysDdns/	GET, POST, PUT, DELETE	DDNS servers
/SysDisclaimer/	GET, PUT	System disclaimer settings
/SysDisclaimer_exclude/	GET, POST, PUT, DELETE	Disclaimer exclusion list
/SysDns/	GET, PUT	System DNS server settings
/SysEncryptionIbe/	GET, PUT	IBE encryption settings
/SysEncryptionIbe_auth/	GET, POST, PUT, DELETE	IBE user authentication list
/SysFortiguard/	GET, PUT	FortiGuard AntiSpam

		settings
/SysFortisandbox/	GET, PUT	FortiSandbox settings
/SysGlobal/	GET, PUT	System global settings
/SysHa/	GET, PUT	HA settings
/SysHaInterface/	GET, PUT	HA interface settings
/SysHaService/	GET, PUT	HA service monitor settings
/SysHaStatus/	GET	HA status
/SysInterface/	GET, POST, PUT, DELETE	Network interface list
/SysLink_monitor/	GET, PUT	Link monitor settings
/SysLink_monitorInterface/	GET, PUT	Link monitor interface settings
/SysMailserver/	GET, PUT	Mail server settings
/SysRemote_mail_server/	GET, POST, PUT, DELETE	Remote email servers
/SysRoute/	GET, POST, PUT, DELETE	Network routing list
/SysSched_backup/	GET, PUT	System configuration scheduled backup settings
/SysScheduledLocalBackup/	GET, PUT	Scheduled local backup list
/SysSnmpCommunity/	GET, POST, PUT, DELETE	SNMP communities
/SysSnmpCommunityHost/	GET, POST, PUT, DELETE	Hosts for a SNMP community
/SysSnmpSnmpv3_user/	GET, POST, PUT, DELETE	SNMP users
/SysSnmpSnmpv3_userHost/	GET, POST, PUT, DELETE	Notification hosts for a SNMP user

/SysSnmpSysinfo/	GET, PUT	SNMP system information settngs
/SysSnmpThreshold/	GET, PUT	SNMP threshold settings
/SysStatisticSummary/	GET	Mail statistics summary
/SysStatusCommand/	POST	Restart / Shut donw / Reload system command
/SysStatusLicinfo/	GET	System AS / AV license status
/SysStatusLicinfoLicenses/	GET	Feature license list
/SysStatusSysinfo/	GET	System status information
/SysStatusUsage/	GET	System resource usage
/SysTimeManual/	GET, PUT	System time & zone settings
/SysTimeNtp/	GET, PUT	System NTP server settings
/SysWccpSettings/	GET, PUT	FortiGate WCCP settings
/UserAlias/ *	GET, POST, PUT, DELETE	User aliases
/UserMail/ *	GET, POST, PUT, DELETE	Mail users
/UserMap/ *	GET, POST, PUT, DELETE	Address maps
/UserPki/	GET, POST, PUT, DELETE	PKI Users
/UserUser_group/ *	GET, POST, PUT, DELETE	User groups

Example commands

Admin login with PKI certificate-based authentication

```
curl -v -c cookie.txt --cert test.pem --key test.key --cacert CA.cer -X
POST -k https://ip_or_host/api/v1/AdminLogin
```

If login is successful, the cookies will be save to cookie.txt, which will be used in the below commands.

Admin login with password-based authentication

```
curl -v -H "Content-Type: application/json" -X POST -d
'{"name":"admin","password":"*****"}' https://ip_or_host/api/v1/AdminLogin
-c cookie.txt
```

If login is successful, the cookies will be save to cookie.txt, which will be used in the below commands.

Note: If your log in to FortiMail with PKI certificate, you must use both the cookie and certificate together to run the command sessions. If you log in with user name and password, you only need to use the cookie to run the command sessions. For example:

To get domain information with password-based authentication

```
curl -k -v  --cookie cookie.txt https://ip_or_host/api/v1/Domain
```

To get domain information with certificate-based authentication

```
curl -k -v  --cookie cookie.txt --cacert CA.cer
https://ip_or_host/api/v1/Domain
```

Access control rule management

Supported values for 'action' attribute of ACL. If not set, the default action is reject.

1 --- safe-relay
2 --- relay
3 --- reject
4 --- discard
5 --- safe

Supported values for 'recipient-pattern-type' and 'sender-pattern-type' attributes of ACL:

0 --- default / wild-card
1 --- regular expression
2 --- email group
3 --- ldap group

Supported values for 'authenticated' attribute of ACL:

0 --- any
1 --- authenticated
2 --- not-authenticated

Supported values for 'sender-ip-type' attribute of ACL:

0 --- ip mask
1 --- ip group

Supported values for 'sortingDirection' attribute of applicable JSON requests (i.e. ACL rule):

1 --- enabled/sorting
2 --- disabled/no sorting

Supported values for 'reqAction' attribute of all JSON requests:

1 --- GET
2 --- CREATE
3 --- DELETE
5 --- UPDATET
14 --- MOVE

Note: If reqAction is present in JSON, it takes precedence over HTTP method header (i.e. HTTP GET/POST/PUT/DELETE).

List Access Control Rules

To list ACL rules in original order:

```
curl -v -b cookie.txt -v -H "Content-Type: application/json" -X PUT -d
'{"reqAction":1,"sortingDirection":2}'
http://ip_or_host/api/v1/MailSetAccessRule
```

To list ACL rules in descending order:

```
curl -v -b cookie.txt -v -H "Content-Type: application/json" -X PUT -d
'{"reqAction":1,"sortingDirection":1}'
http://ip_or_host/api/v1/MailSetAccessRule
```

Create a new Access Control Rule

```
curl -v -H "Content-Type: application/json" -X POST -d
'{"status":true,"sender_pattern":"*@example.com","sender_ip_mask":"192.168.
1.1/32", "action":2}' -b cookie.txt
http://ip_or_host/api/v1/MailSetAccessRule/0
--No mkey is required
```

Modify an existing Access Control Rule

```
curl -v -H "Content-Type: application/json" -X PUT -d '{"action":3}' -b
cookie.txt http://ip_or_host/api/v1/MailSetAccessRule/1
--"1" is the mkey
--Set access rule "1" action to "Reject"
```

Delete an existing Access Control Rule

```
curl -v -H "Content-Type: application/json" -X DELETE -b cookie.txt
http://ip_or_host/api/v1/MailSetAccessRule/3
--Delete Access Control Rule "3"
```

Move existing Access Control Rules

You can move a rule up one place, down one place, before another rule, or after another rule. To move a rule to the top or bottom, you can find the first. or last rule ID (mkey) and move the rule before the first rule or after the last rule.

reqAction: 14 -- required, only one value: 14 means to move

moveAction : up -- required, 4 values: up/down/before/after

mmkey: 3 – required, ID of the ACL rule to be moved

refMkey: 2 – required, reference ID of the ACL rule when moving before/after this ID

To move rule"3" up one place:

```
curl -v -H "Content-Type: application/json" -X PUT -d
'{"reqAction":"14","mmkey":3,"moveAction":"up"}' -b cookie.txt
http://ip_or_host/api/v1/MailSetAccessRule
```

To move rule "3" after rule "2":

```
curl -v -H "Content-Type: application/json" -X PUT -d
'{"reqAction":"14","mmkey":3,"moveAction":"after",”refMkey”:2}' -b
cookie.txt http://ip_or_host/api/v1/MailSetAccessRule
```