c

FORTINET
High Performance Network Security

FortiMail™Cloud QuickStart Guide

VERSION 1.0

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

May 21, 2020

FortiMail™ Cloud QuickStart Guide

TABLE OF CONTENTS

Document scope

This document is the copyright of Fortinet, Inc. (“Fortinet”), and is intended for internal use and Customer distribution only. Service in this document is defined as any combination of the various services outlined below and ordered by the Customer (“Service“).

The purpose of this document is to provide initial setup guidance when deploying FortiMail Cloud. It includes initial configuration and testing of any protected domains. Customers should consult their Fortinet Sales Engineer (SE) for any questions that arise as a consequence of these instructions, who may direct them to contact the Fortinet Support teams where necessary.

Please note that any advanced configuration should be undertaken utilizing the FortiMail Administration Guide, which can be located at http://docs.fortinet.com.

About FortiMail Cloud

FortiMail Cloud Email Security is an independently validated and top-rated Secure Email Gateway solution delivering >99% catch rate, multiple layers of malware detection and an extremely low false positive rate. Fully managed by Fortinet, FortiMail Cloud allows the customer to focus on business goals by relying on a trusted security expert to manage this key infrastructure security component.

FortiMail Cloud is available in 2 different deployment options:

- **Gateway** — Route email to Fortinet where it is cleaned of malware and spam and forwarded onwards to existing customer mail servers.
- **Server** — Hosted email infrastructure and security with Fortinet while benefiting from malware and spam protection as well as protection of sensitive information.

Additionally, for both deployments, FortiMail Cloud has a ‘Premium’ option, which adds Data Loss Prevention, Identity Based Encryption and Sandboxing. For the Server offering, the Premium service also adds additional mailbox storage.

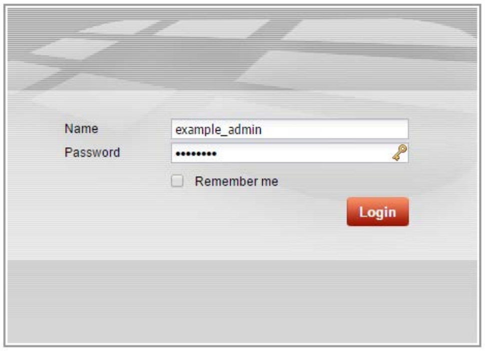
This guide is written on the assumption the customer is deploying the service in Gateway mode, and will be continuing to deliver email to their own email architecture, whether on premises or within a cloud environment.

Logging on to FortiMail Cloud

Upon receipt of your documentation, this should include the information for the URL to connect to your FortiMail Cloud, as well as a preconfigured administrator username and password. If you have not received this information, please contact your distributor in the first instance.

Your FortiMail Cloud environment will be preconfigured with the detail provided in the FortiMail Cloud Provisioning Template, including the number of Protected Mailboxes and the names of the Protected Domains involved.

As part of your documentation, you will be provided with the URL for your FortiMail Cloud service, in the format **https://gwxxx.fortimail.com/admin.** When first logging in, you will be prompted for the Administrator details that were provided. Once completed, this portal will connect you to the GUI of your FortiMail Cloud unit.



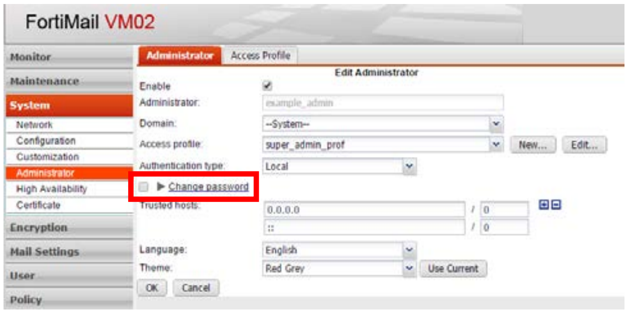
Name: example_admin

Password: ••••••••

□ Remember me

Changing the administrator password

The designated administrators of the FortiMail Cloud platform will be sent user credentials to log on to the service. It is highly recommended that you change these at first login under ***System > Administrator***.



Edit Administrator

Enable: ☑

Administrator: example_admin

Domain: --System--

Access profile: super_admin_prof

Authentication type: Local

□ ▶ Change password

Trusted hosts: 0.0.0.0 / 0

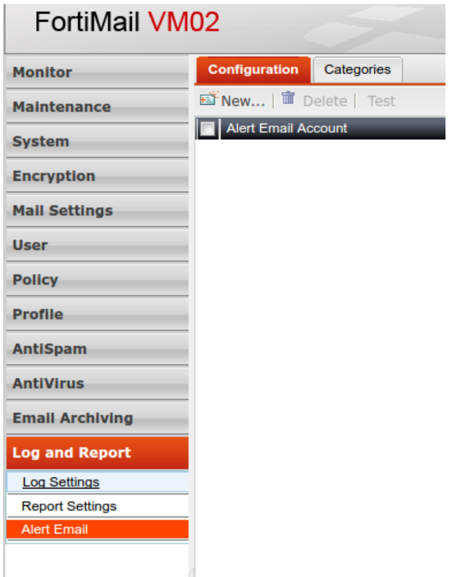
:: / 0

Language: English

Theme: Red Grey

Checking alert email settings

If provided in the initial configuration template, the Alert Email address for monitoring and alerting will have already been configured when the unit is provisioned. Fortinet recommends customers check this setting to ensure any alerts are being forwarded properly. You can locate this under ***Log and Report > Alert Email.***



Best practice configuration

The FortiMail Cloud environment is configured with a basic, "Best Practice" configuration that has been set up to provide a basic anti-Spam, anti-virus and anti-malware configuration, but is not initially customized for a customer environment.

Fortinet recommends that before utilizing the environment, the customer reviews these default settings to ensure they meet their organizations filtering and control requirements, as well as meeting any organizational or regulatory compliance demands.

Configuring inbound email relay

To enable email to be forwarded from FortiMail Cloud, the instance must be configured with the necessary information of your existing email server infrastructure.

To do this from the GUI:

- Mail Settings
  - Domain
    - Edit Domain: <example.com>
    - Choose Relay Type: <Click the ? Icon to describe available relay types>
  - SMTP Server
    - IP Address or DNS Name*
    - Port
  - Fallback SMTP Server (Optional, Recommended)

- IP Address or DNS Name*
- Port

***Note**: DNS Names used for SMTP & Fallback SMTP must be different from those used for the delivery of your service, to avoid routing loops.*

Testing inbound email relay prior to updating MX records

Fortinet recommends prior to migrating any organizational email to FortiMail Cloud, testing is conducted to ensure your FortiMail Cloud unit can successfully deliver incoming email to a test user, without altering the public DNS MX record.

The configuration required to achieve this may vary depending on the exact mail server in use by the organization, for the purposes of this documentation a Linux host with shell access is used. In order to complete this test, you will need to create the mailbox ‘testuser’ to ensure delivery.

Lines with -->> are commands that will need to be entered as part of the test (Do not enter the -->> text.). Other lines show the appropriate response. Replace instances of **gwxxx.fortimail.com** with the addressing information provided for login.

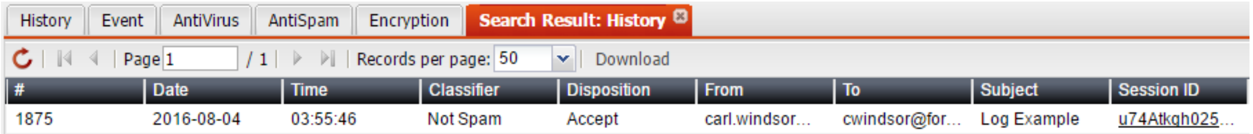
To test with CLI commands:

```
-->>telnet gwxxx.fortimail.com 25

220 gwxxx.fortimail.com ESMTP Smtpd; [Date and Time]

-->>ehlo

250-gwxxx.fortimail.com Hello linuxhost.example.com [public ip of linuxhost.example.com], pleased to meet you

250-ENHANCEDSTATUSCODES

250-PIPELINING

250-8BITMIME

250-SIZE 10485760

250-DSN

250-STARTTLS

250-DELIVERBY

250 HELP

-->>mail from: <testuser@example.com>
```

```
250 2.1.0 <testuser@example.com>... Sender ok

-->>rcpt to: <testuser@example.com>

250 2.1.5 <testuser@example.com>... Recipient ok

-->>data

354 Enter mail, end with "." on a line by itself

-->>Subject: Test

-->>Test

-->>.

-->>quit

250 2.0.0 u0XXXXXX000000-u0XXXXXX000000 Message accepted for delivery

221 2.0.0 gwxxx.fortimail.com closing connection

Connection closed by foreign host
```

***Note**: It is important that the test user you are using actually exists on your server. Emails addressed to non-existing users can be rejected either by your server or by the FML cloud unit if recipient address verification is enabled.*

Check the mailbox of the user "testuser@example.com" to see if the server has received the Email. You can also check the FortiMail Cloud log to see whether this email is successfully delivered. This can be found under ***Monitor > Log > History***.



#	Date	Time	Classifier	Disposition	From	To	Subject	Session ID
1875	2016-08-04	03:55:46	Not Spam	Accept	carl.windsor...	cwindsor@for...	Log Example	u74Atkgh025...

If the Email has not been received, refer to the FortiMail Cloud logs to identify the reason and modify your configuration or tests accordingly. The most common cause for this error is misconfiguration of the relaying Email server above. In the first instance, Fortinet recommends validating the information previously configured in *“7. Configure inbound Email relaying"*.

Updating the MX record, SPF record and testing incoming email

In this step, you will change your public MX record to the hostname of the FortiMail Cloud unit and test incoming emails. Incoming emails to your Domain from the public Internet are delivered to the host of the public MX record for your domain.

Please note immediately after you change your public MX record, incoming Emails to your Domain will begin to be routed to the FML cloud unit, dependent on the Time To Live (TTL) of the DNS entry. The mechanisms for updating your MX record are dependent on your DNS hosting provider, and are outside of the scope of this document.

***Note**: It is highly recommended that prior to undertaking the following steps that customers shorten the TTL of their MX records prior to migration and during testing. Failure to do this can result in prolonged downtime of your Email architecture in the event of troubleshooting of the configuration.*

Updating the MX record and SPF record

Assuming your current public MX record is:

example.com. 86400 IN MX 10 mail.example.com.

Change it to:

example.com. 86400 IN MX 10 gwxxx.fortimail.com.

Email from the public Internet will now begin to be forwarded to your FortiMail Cloud.

Assuming you SPF record is:

```
v=spf1 ip4:x.x.x.x a:mail.example.com include:example.com -all
```

Change it to:

```
v=spf1 ip4:x.x.x.x a:gwxxx.fortimail.com include:example.com -all
```

Where example.com is your mail domain and the IPv4 address is the same as the A record of gwxxx.fortimail.com.

Testing inbound email delivery

Send a test email to the test user created earlier, *"testuser@example.com"*. You can use any current email client you are using or public Webmail service to achieve this. It is important that the host you are using to send the email can correctly resolve the public MX record of your domain.

If testing using a shell on a Linux host, please change the telnet command to: **telnet example.com 25.**

At this point, check the mailbox of the user "testuser@example.com" to see if the Email has been received. You can also check FortiMail Cloud Unit log to see whether this email is successfully delivered, and capture further information.

Configuring outbound email

The FortiMail Cloud service by default is configured to provide services for inbound email. But it can also if desired be configured to provide the same level of access control for outbound email. This requires you to configure equivalent access policies as previously for Inbound service, and is beyond the scope of this QuickStart Guide.

Please refer to the full FortiMail Administration Guide should this be necessary.

***Note**: Extra care must be taken when configuring outbound relaying from your existing Email architecture. Misconfiguration of this step can result in an ‘Open Relay’, enabling external parties to send & receive Email as if part of your organization.*

Summary

At this point, you should be able to send and receive email through your FortiMail Cloud environment, and have full access to create, delete and modify policies according to the security requirements of your organization. Fortinet recommends that users wishing to make further customization do so by reviewing the FortiMail Administration Guide, which can be located at http://docs.fortinet.com.

Further training and guidance are also available. Please contact your respective reseller or support channel as appropriate.

FORTINET®

High Performance Network Security