



# FortiMail Cloud - QuickStart Guide

Version 6.4.0

**FORTINET DOCUMENT LIBRARY**

<https://docs.fortinet.com>

**FORTINET VIDEO GUIDE**

<https://video.fortinet.com>

**FORTINET BLOG**

<https://blog.fortinet.com>

**CUSTOMER SERVICE & SUPPORT**

<https://support.fortinet.com>

**FORTINET TRAINING & CERTIFICATION PROGRAM**

<https://www.fortinet.com/support-and-training/training.html>

**NSE INSTITUTE**

<https://training.fortinet.com>

**FORTIGUARD CENTER**

<https://fortiguard.com/>

**END USER LICENSE AGREEMENT**

<https://www.fortinet.com/doc/legal/EULA.pdf>

**FEEDBACK**

Email: [techdoc@fortinet.com](mailto:techdoc@fortinet.com)



June 26, 2020

FortiMail Cloud 6.4.0 QuickStart Guide

06-640-000000-20200626

# TABLE OF CONTENTS

<b>Change Log</b> .....	<b>4</b>
<b>Document scope</b> .....	<b>5</b>
<b>About FortiMail Cloud</b> .....	<b>6</b>
<b>Logging on to Fortimail Cloud</b> .....	<b>7</b>
<b>Changing the administrator password</b> .....	<b>8</b>
<b>Checking alert email settings</b> .....	<b>9</b>
<b>Best practice configuration</b> .....	<b>10</b>
<b>Configuring inbound email relay</b> .....	<b>11</b>
Testing inbound email relay prior to updating MX records .....	11
<b>Updating the MX record, SPF record, and testing inbound email</b> .....	<b>13</b>
Updating the MX record and SPF record .....	13
Testing inbound email delivery .....	13
<b>Configuring outbound email</b> .....	<b>15</b>
<b>Summary</b> .....	<b>16</b>

# Change Log

Date	Change Description
2020-06-26	Initial release.

# 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 <https://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 two 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 (DLP), Identity Based Encryption (IBE) 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.

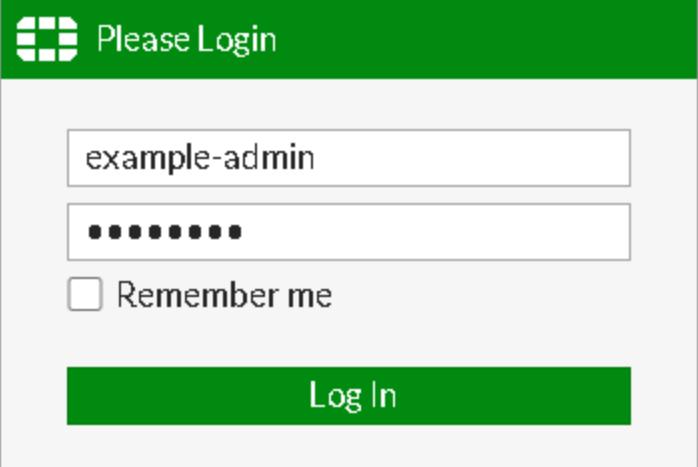
---

# 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.



Please Login

example-admin

••••••••

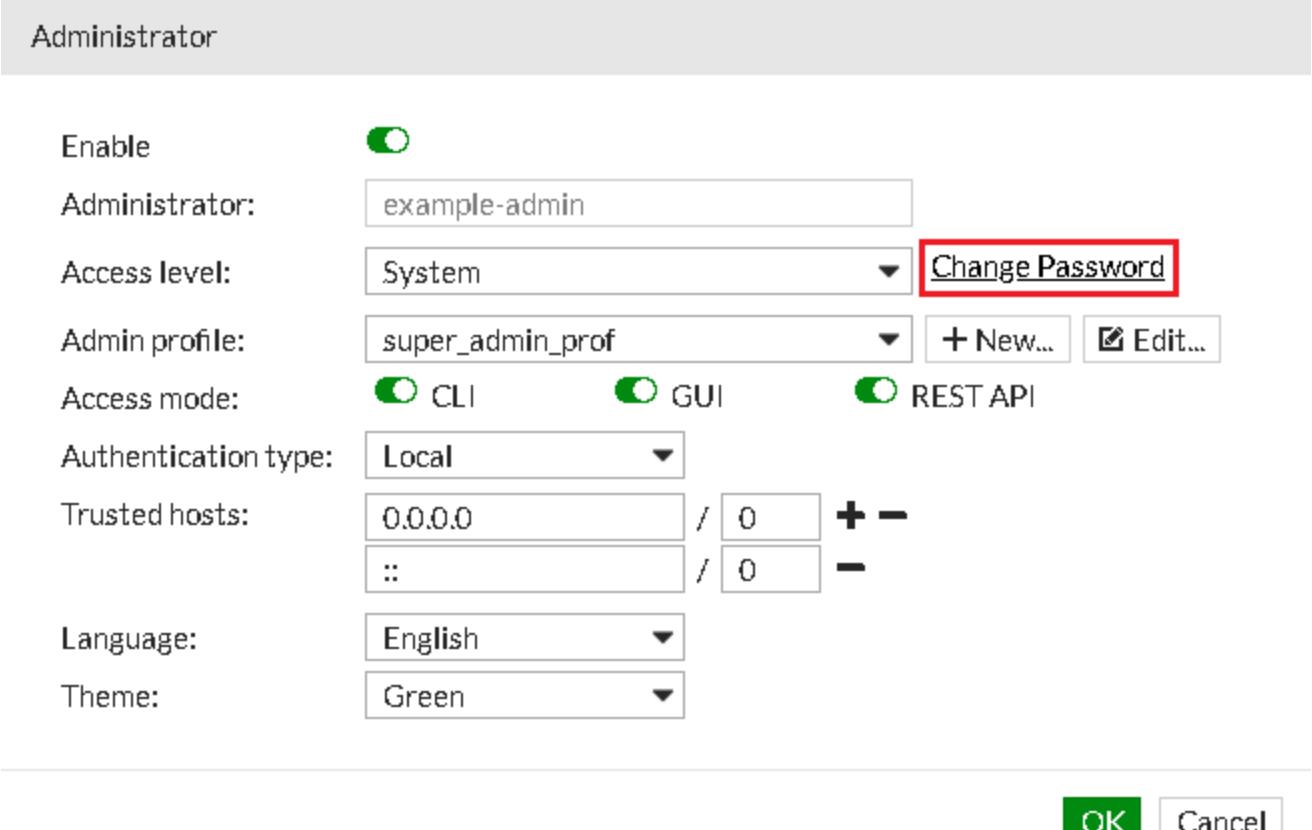
Remember me

Log In

# 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 > Administrator*, edit the administrator account and click *Change Password*.



The screenshot shows the 'Administrator' configuration dialog. The 'Enable' switch is turned on. The 'Administrator' field contains 'example-admin'. The 'Access level' dropdown is set to 'System' and has a 'Change Password' button to its right, which is highlighted with a red box. The 'Admin profile' dropdown is set to 'super\_admin\_prof' with a '+ New...' and 'Edit...' button to its right. Under 'Access mode', 'CLI' and 'GUI' are selected, while 'REST API' is not. The 'Authentication type' dropdown is set to 'Local'. The 'Trusted hosts' section shows '0.0.0.0 / 0' and ':: / 0' with '+ -' and '-' buttons respectively. The 'Language' dropdown is set to 'English' and the 'Theme' dropdown is set to 'Green'. At the bottom are 'OK' and 'Cancel' buttons.

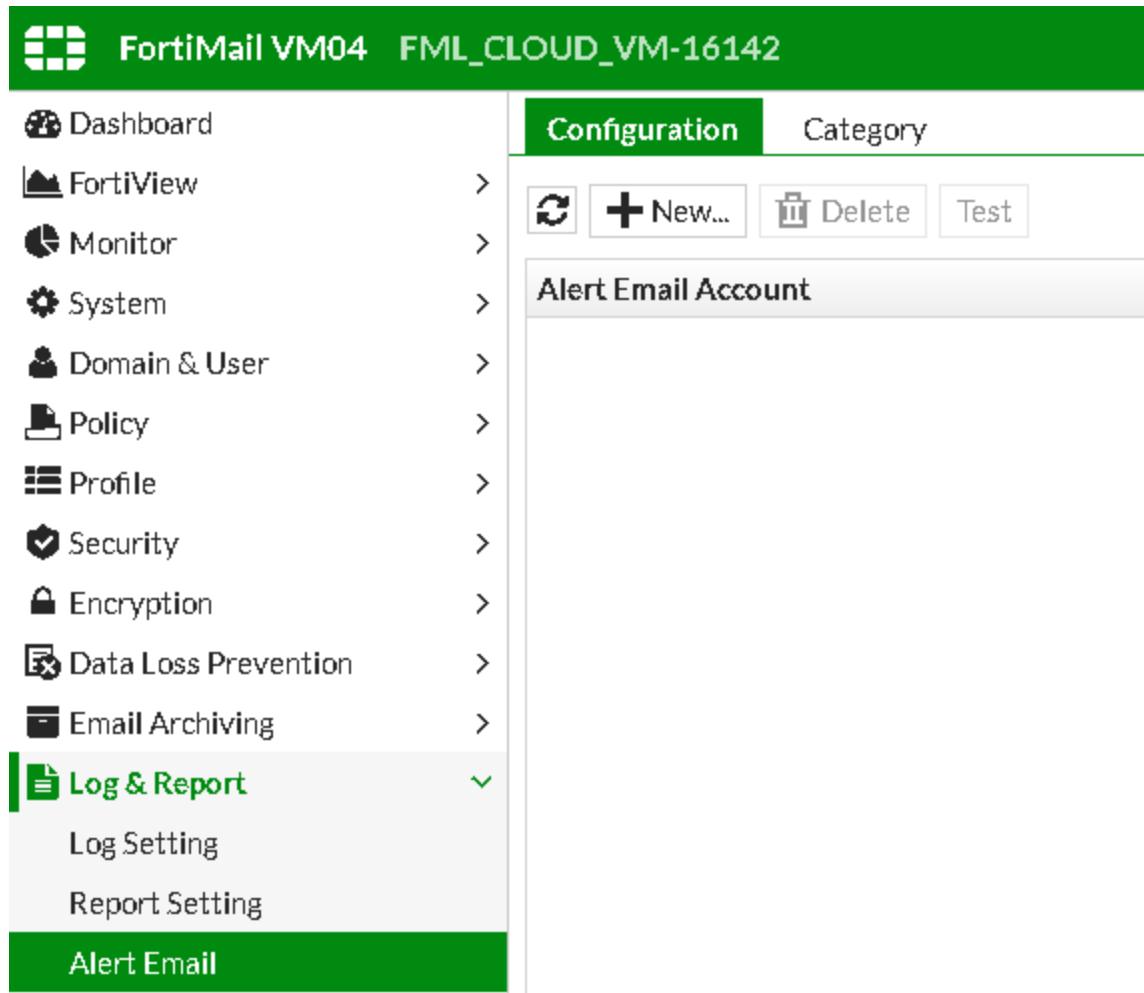
Administrator:	example-admin		
Access level:	System	Change Password	
Admin profile:	super_admin_prof	+ New... Edit...	
Access mode:	CLI	GUI	REST API
Authentication type:	Local		
Trusted hosts:	0.0.0.0 / 0	+ -	
	:: / 0	-	
Language:	English		
Theme:	Green		

OK Cancel

# 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 & Report > Alert Email > Configuration* and *Log & Report > Alert Email > Category*.



The screenshot shows the FortiMail VM04 interface with the title bar "FortiMail VM04 FML\_CLOUD\_VM-16142". The left sidebar menu includes: Dashboard, FortiView, Monitor, System, Domain & User, Policy, Profile, Security, Encryption, Data Loss Prevention, Email Archiving, Log & Report (selected), Log Setting, Report Setting, and Alert Email (selected). The main content area has tabs "Configuration" and "Category" (selected). Below the tabs are buttons for Refresh, New, Delete, and Test. The "Alert Email Account" section is displayed, showing a table with columns for Name, Type, and Status. The table contains one row: "Alert Email Account" (Type: Email, Status: Enabled).

## 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 forward email from FortiMail Cloud:

1. Go to *Domain & User > Domain > Domain* and create a new domain or edit an existing domain.
2. Configure the information as necessary, providing the IP address or DNS name and port of your SMTP server (and optionally fallback SMTP server).

For more detailed information, see the Configuring protected domains section of the [FortiMail Administration Guide](#).



DNS names used for SMTP and 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 u0XXXXXXXX000000-u0XXXXXXXX000000 Message accepted for delivery
221 2.0.0 gwxxx.fortimail.com closing connection
Connection closed by foreign host
```

---



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 FortiMail 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 under *Monitor > Log > History* and using the *Search* option.

The screenshot shows the 'Log History' section of the FortiMail Cloud interface. The top navigation bar includes tabs for History, System Event, Mail Event, AntiVirus, AntiSpam, Encryption, History Log Search (which is selected and highlighted in green), and a search bar. Below the navigation is a search and filter bar with fields for Date, Time, Classifier, Disposition, From, To, Subject, and Session ID, along with buttons for View and Download. The main area displays a table of log entries. The first column is labeled '#', and the other columns are Date, Time, Classifier, Disposition, From, To, Subject, and Session ID. The first log entry is partially visible, showing a timestamp of '2023-01-12 10:00:00' and a subject of 'Test'.

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 [Configuring inbound email relay](#).

# Updating the MX record, SPF record, and testing inbound 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 FortiMail 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.



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

### Example public MX record:

```
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.

### Example SPF record:

```
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 [FortiMail Administration Guide](#) should this be necessary.



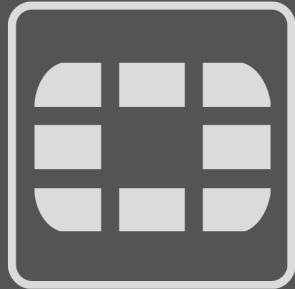
Extra care must be taken when configuring outbound relaying from your existing email architecture. Misconfiguration of this step can result in an "Open Relay", enabling external parties to send and receive email as if part of your organization.

---

# 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 <https://docs.fortinet.com>.

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



Copyright© 2020 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.