FortiMail Cloud User Portal Guide

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 COOKBOOK

https://cookbook.fortinet.com

FORTINET TRAINING SERVICES

https://www.fortinet.com/training

FORTIGUARD CENTER

https://www.fortiguard.com

END USER LICENSE AGREEMENT

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

FEEDBACK

Email: techdocs@fortinet.com

January 11, 2024

TABLE OF CONTENTS

Change Log 4
Introduction 5
Accessing the user portal 5

Change Log

Date	Change Description
2024-01-11	Initial release.

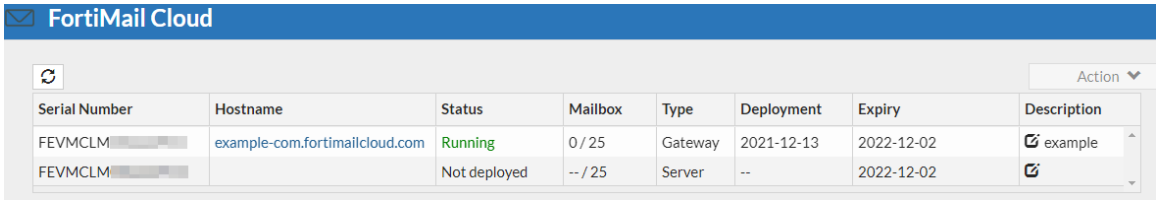
Introduction

Fortinet (NASDAQ: FTNT) FortiMail Cloud delivers email security as a managed service to businesses based around the globe. FortiMail Cloud is a complete Secure Email Gateway platform that protects against inbound attacks, including advanced malware, as well as outbound threats and data loss, operating from multiple geographical data centers.

This document outlines operation of the FortiMail Cloud User Portal, which allows customers to manage their running FortiMail Cloud instances from a single place.

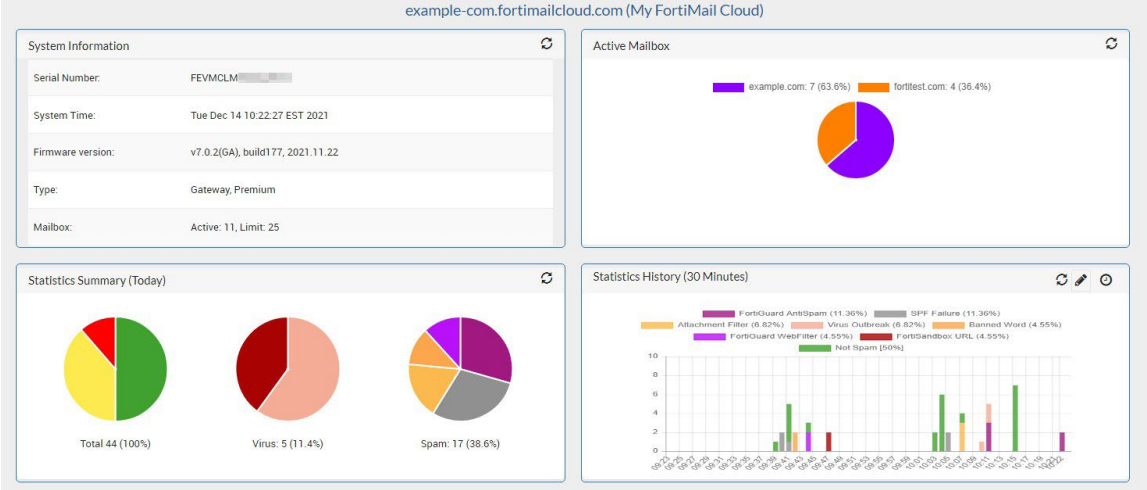
Accessing the user portal

1. Go to https://support.fortinet.com, click **Register** to create a FortiCloud account. If you already have one, please login with your account.
2. Once you entered your account, please register a product with the contract registration code. Please follow the registration process until complete, and a serial number of your FortiMail Cloud license is provided.
3. Click "**FortiMail**" under **Services > Cloud Services** to access the FML Cloud User Portal, otherwise, you can also access directly to https://www.fortimailcloud.com and select "Log In".
4. You will find all your registered licenses listed with the status "**Not deployed**" or "**Running**". Additional information of your FortiMail license is shown in the table, such as "**Serial Number**", "**Registered Mailbox Number**" and "**License Type**".

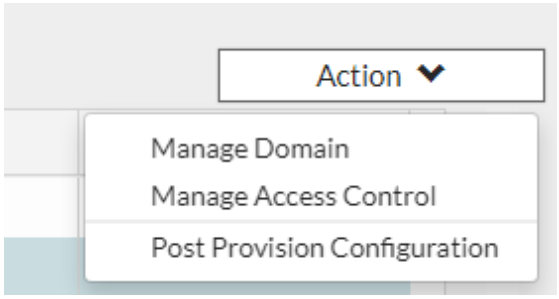


5. For the "**Not deployed**" licenses, please go to https://support.fortinet.com to create a ticket for provisioning request, and check the instance status again once get notified that your FortiMail Cloud instance is provisioned.
6. For "**Running**" instances, please click on the link under "**Hostname**" to access to your FortiMail Cloud instance. You will log in automatically and no password is needed.

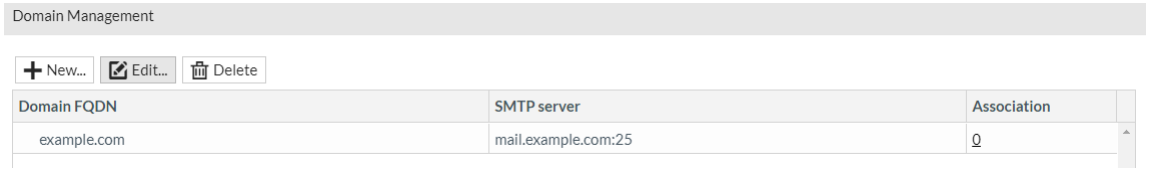
7. Once an instance is provisioned, you can click to select it. Further status is displayed on the user portal: “**System Information**”, “**Active Mailbox**”, “**Statistics Summary and History**”. You can get more details in the FortiMail Admin GUI.



8. You can also select a “**Running**” instance which will make the button “**Action**” available (upper right corner), and choose from the menu: “**Manage Domain**”, “**Manage Access Control**” and “**Post Provision Configuration**”.



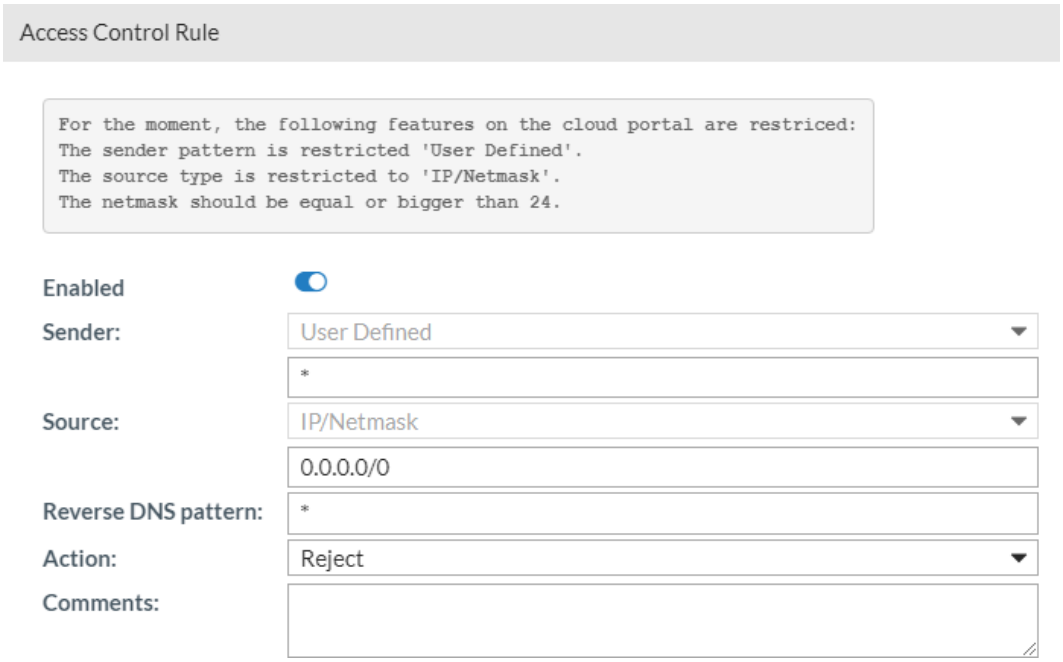
9. You can edit the SMTP server or port for an existing domain or add a new domain.



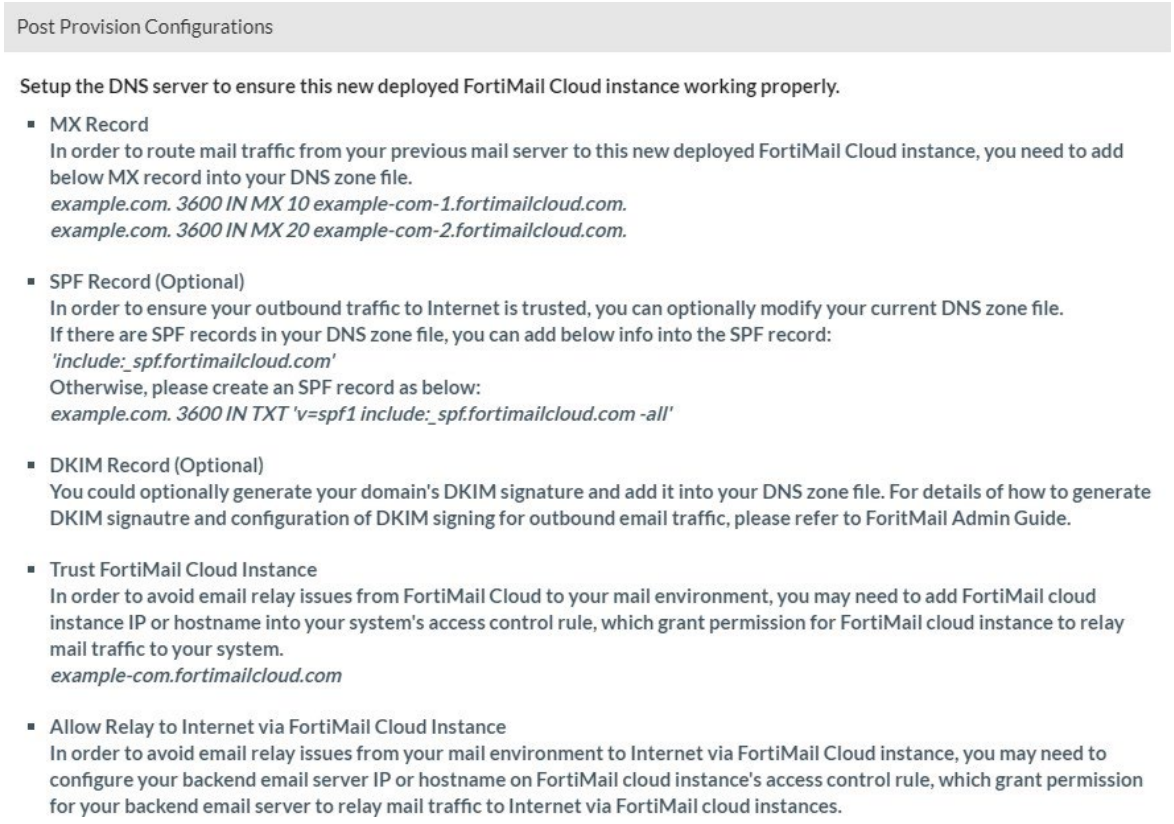
Please note that you're not able to do such actions in FortiMail Admin GUI.

Besides, the Domain Ownership Verification is required each time you want to add a new domain on your FortiMail.

10. You can add or edit an Access Control Rule through the Cloud user portal. Please note, there are additional restrictions as per below;



11. The section “**Post Provision Configuration**” shows some guides to modify your DNS records or the policy on your other systems. You can find the same guides in the Welcome email (which notifies you the FortiMail instance is provisioned).



Post Provision Configurations

Setup the DNS server to ensure this new deployed FortiMail Cloud instance working properly.

- MX Record
  In order to route mail traffic from your previous mail server to this new deployed FortiMail Cloud instance, you need to add below MX record into your DNS zone file.
  example.com. 3600 IN MX 10 example-com-1.fortimailcloud.com.
  example.com. 3600 IN MX 20 example-com-2.fortimailcloud.com.

- SPF Record (Optional)
  In order to ensure your outbound traffic to Internet is trusted, you can optionally modify your current DNS zone file.
  If there are SPF records in your DNS zone file, you can add below info into the SPF record:
  'include:_spf.fortimailcloud.com'
  Otherwise, please create an SPF record as below:
  example.com. 3600 IN TXT 'v=spf1 include:_spf.fortimailcloud.com -all'

- DKIM Record (Optional)
  You could optionally generate your domain's DKIM signature and add it into your DNS zone file. For details of how to generate DKIM signautre and configuration of DKIM signing for outbound email traffic, please refer to ForitMail Admin Guide.

- Trust FortiMail Cloud Instance
  In order to avoid email relay issues from FortiMail Cloud to your mail environment, you may need to add FortiMail cloud instance IP or hostname into your system's access control rule, which grant permission for FortiMail cloud instance to relay mail traffic to your system.
  example-com.fortimailcloud.com

- Allow Relay to Internet via FortiMail Cloud Instance
  In order to avoid email relay issues from your mail environment to Internet via FortiMail Cloud instance, you may need to configure your backend email server IP or hostname on FortiMail cloud instance's access control rule, which grant permission for your backend email server to relay mail traffic to Internet via FortiMail cloud instances.

Copyright© 2024 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.