FortiMail: Configuration Best Practices

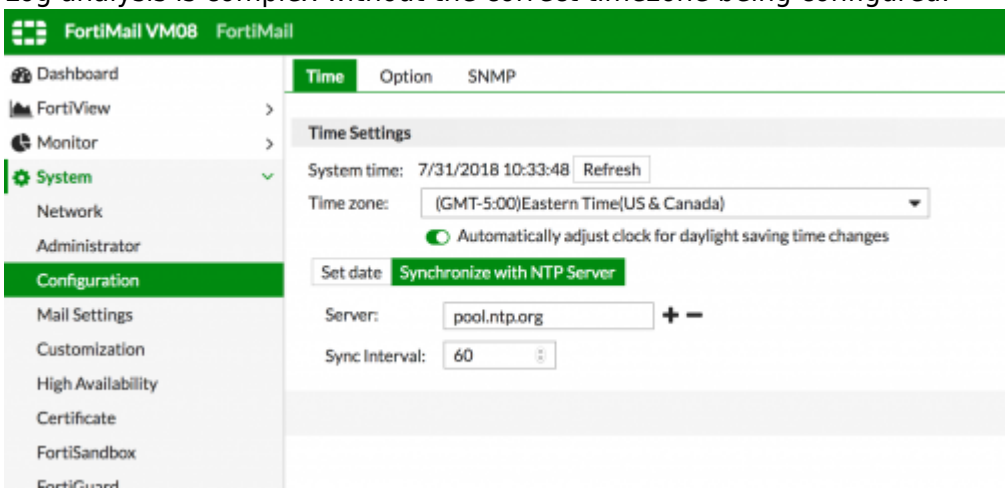
This page presents best practice configuration items for FortiMail and is organized by topic.

Best practices are intended to be encompassing of most environments. The user is however expected to assess the recommendations and gain an understanding of whether they are correct in his specific use case.

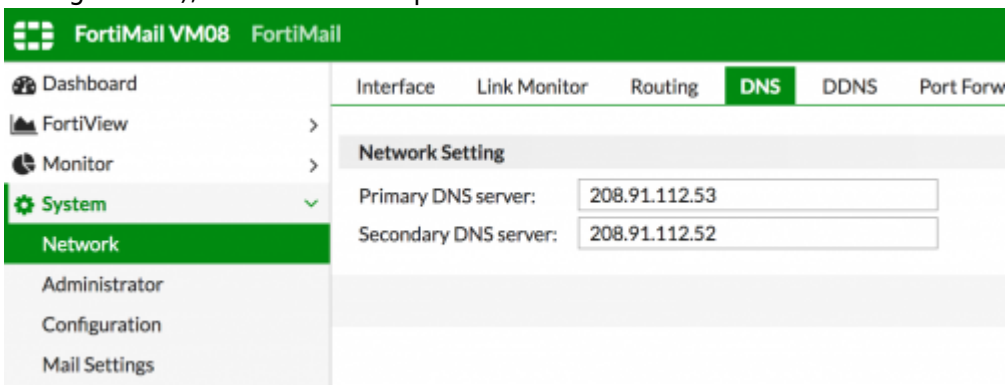
Network and base configuration

Setup date and time parameters

Log analysis is complex without the correct timezone being configured.



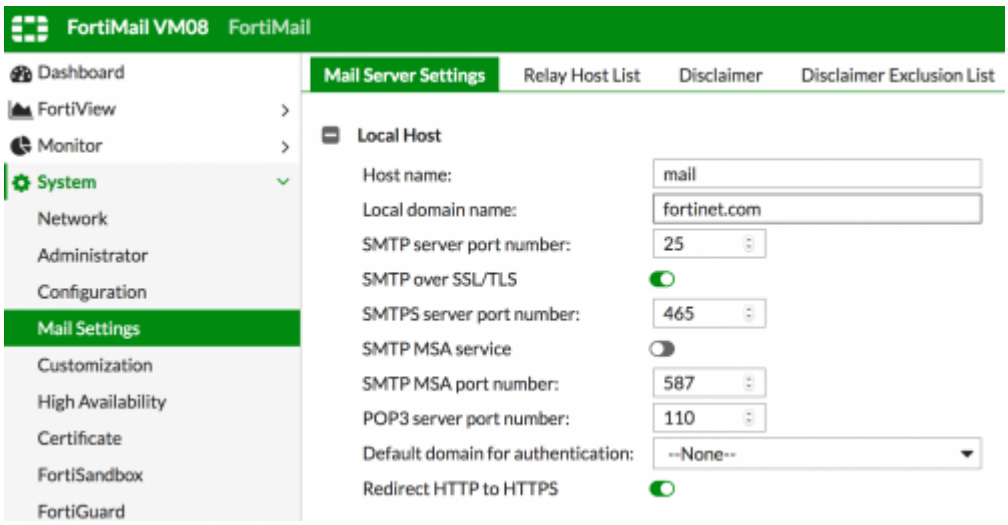
Setup forward DNS Setup forward DNS to organization standard DNS, keeping in mind that DNS is used for a number of controls and if internal zone queries are needed (e.g. usage of internal hostnames in the configuration), the unit should point to recursive servers that can resolve those.



MTA Parameters

Setup hostname and local domain name

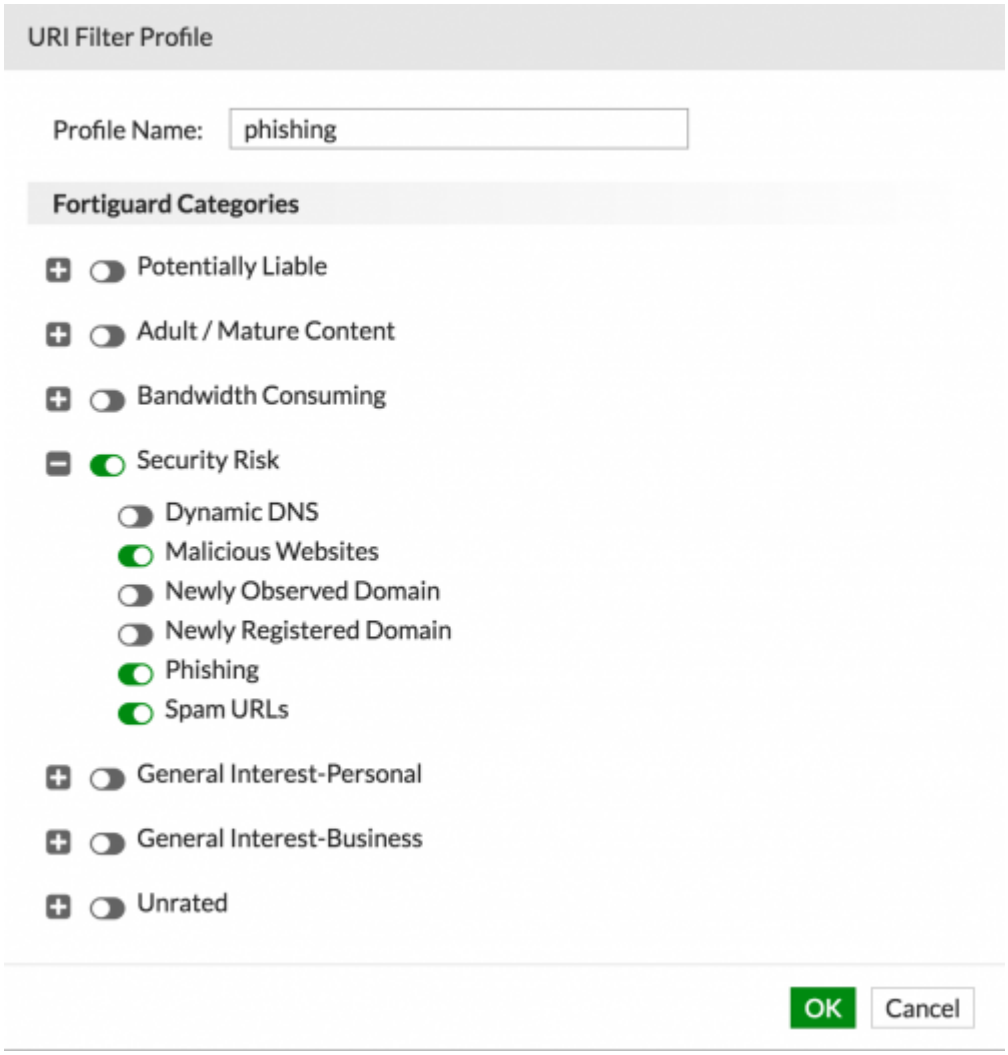
This information is used by the MTA as its identity for both incoming and outgoing SMTP connection. It should be set to a hostname for which forward lookup points to the FortiMail public IP address used for establishing outbound connections.

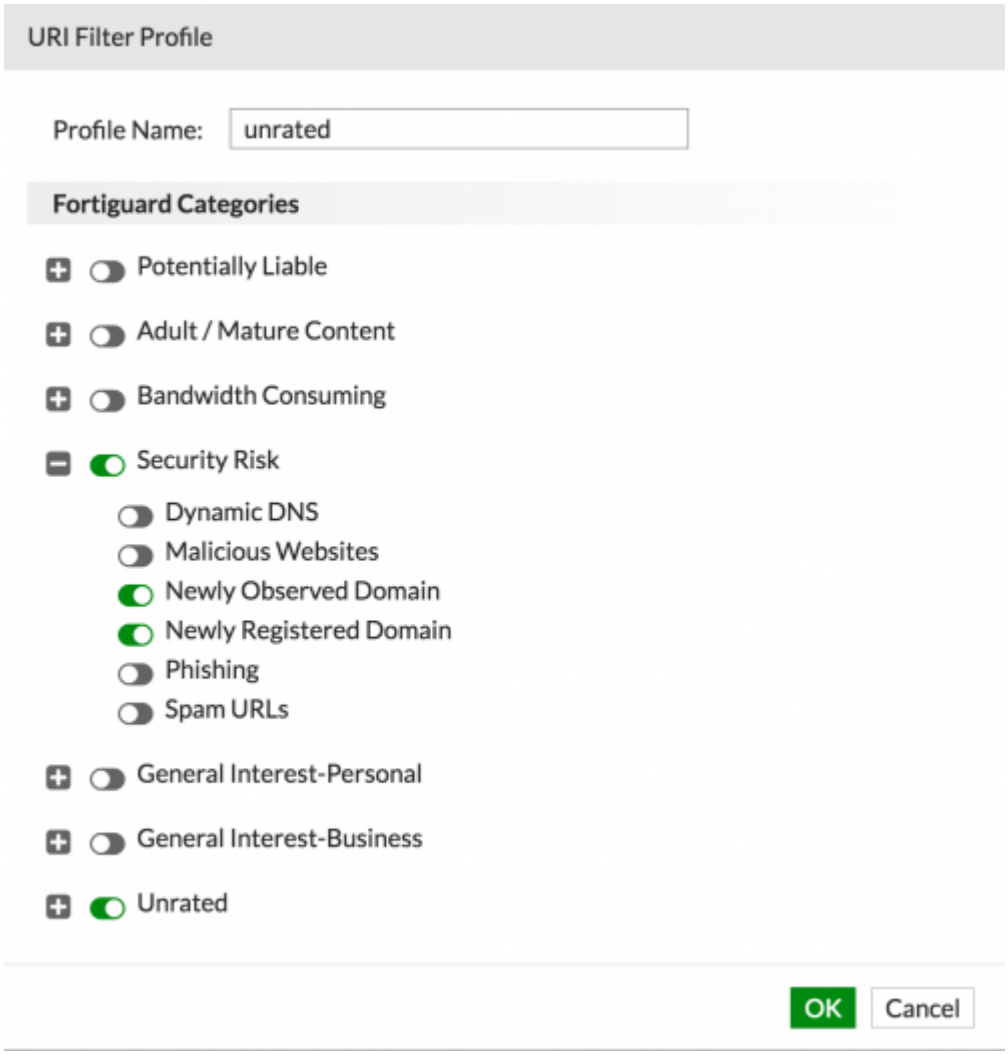


Security Profiles

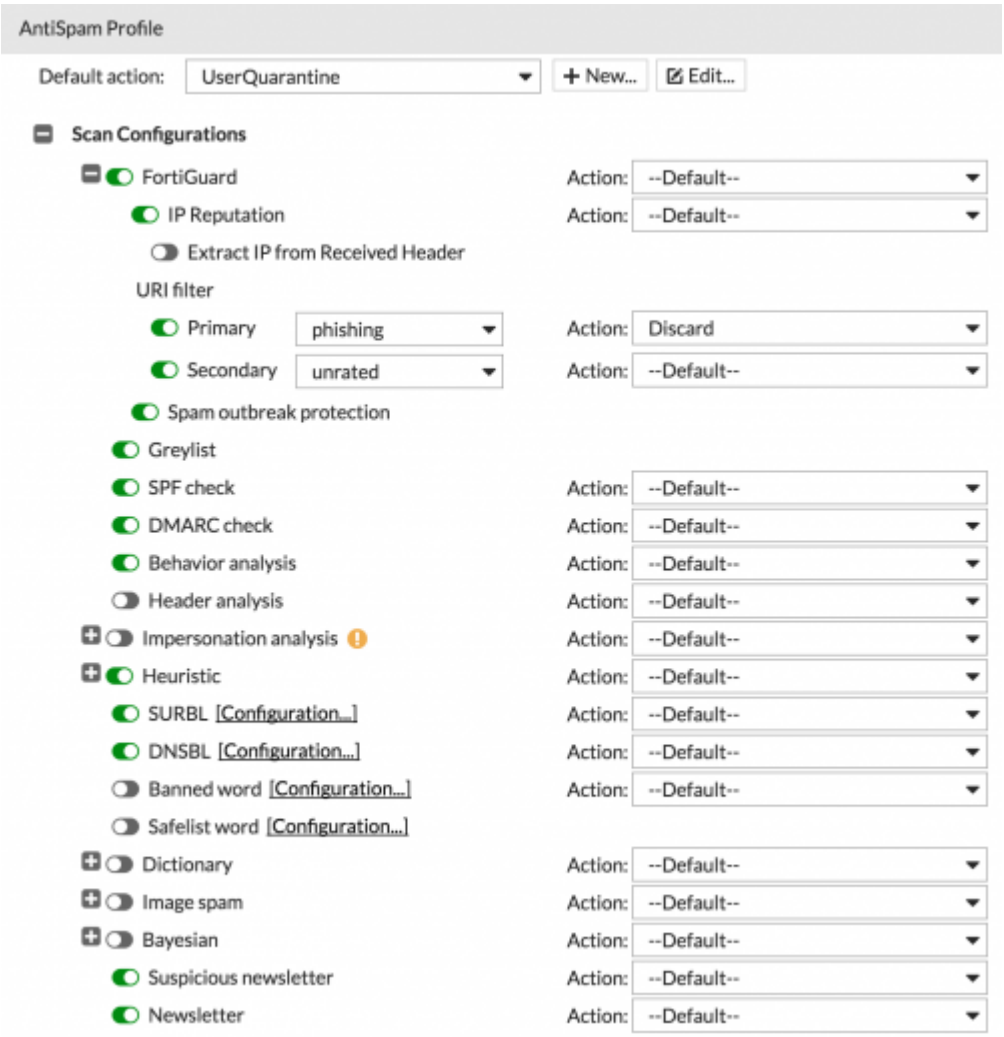
Antispam profile: generally recommended settings

Configure two URI filter profiles, or edit existing default profiles “phishing” and “unrated” to ensure they match the following:


URI Filter Profile
Profile Name:
phishing
Fortiguard Categories
Potentially Liable
Adult / Mature Content
Bandwidth Consuming
Security Risk
Dynamic DNS
Malicious Websites
Newly Observed Domain
Newly Registered Domain
Phishing
Spam URLs
General Interest-Personal
General Interest-Business
Unrated
OK
Cancel



The following screenshot shows the default recommended options for inbound antispam filtering:



Do note that two controls in this list can result in email delivery delay:

- Greylisting: will delay delivery the first time we see a sender, but not afterwards
- Spam outbreak protection: may delay delivery when emails as perceived as suspicious

This recommendation assumes that user quarantine is being leveraged. If not desired, system quarantine can be used instead.