FortiMail - Cookbook

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

May 8, 2020
FortiMail 6.4.0 Cookbook
06-640-000000-20200508

TABLE OF CONTENTS

Change Log

Date	Change Description
2020-05-08	Initial release.

AntiSpam

This section contains information about configuring antispam related features.

Configuring adult image analysis in FortiMail

Maybe you suspect an employee of viewing adult images or videos during office hours through his or her email. Maybe you’re receiving unsolicited adult files through your email. In either scenario, FortiMail can help you keep your office setting professional through a new scanning option that detects if an email contains adult sensitive material.

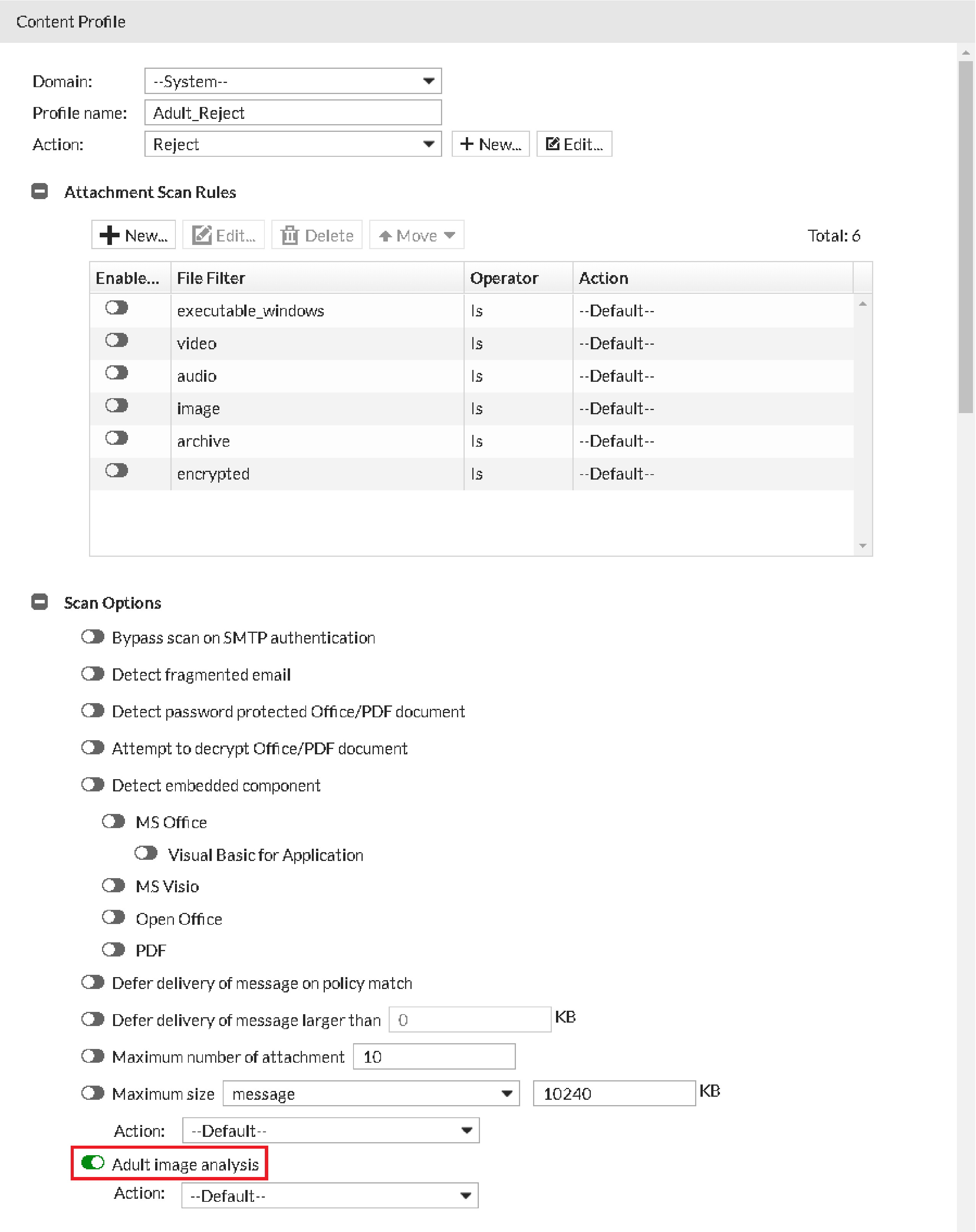
In this recipe, you will configure a content profile to scan for adult images in the email body and attachments.

Configuring a Content Profile and Scan Options

For this recipe we’ll need to briefly go over the content profile creation process. If you would like a more detailed explanation, see the content profile section in the FortiMail Administrator Guide.

1. Go to **Profile > Content > Content** and click **New**, or edit an existing profile.
2. If creating a new profile, and there are multiple domains, select whether the profile is used system-wide or for a specific domain from the **Domain** drop-down menu.
3. Enter a **Profile name**.
4. Set **Action** to **Reject**. This profile will make FortiMail reply to the SMTP client with SMTP reply code 550. All emails containing adult images will be rejected.
5. Under **Scan Options**, enable **Adult image analysis**. Leave the **Action** set to **Default**. You will determine the

default actions of adult image analysis in the next step.



Content Profile

Domain: --System--

Profile name: Adult_Reject

Action: Reject

Attachment Scan Rules

Total: 6

Enable...	File Filter	Operator	Action
○	executable_windows	Is	--Default--
○	video	Is	--Default--
○	audio	Is	--Default--
○	image	Is	--Default--
○	archive	Is	--Default--
○	encrypted	Is	--Default--

Scan Options

- ○ Bypass scan on SMTP authentication
- ○ Detect fragmented email
- ○ Detect password protected Office/PDF document
- ○ Attempt to decrypt Office/PDF document
- ○ Detect embedded component
  - ○ MS Office
    - ○ Visual Basic for Application
  - ○ MS Visio
  - ○ Open Office
  - ○ PDF
- ○ Defer delivery of message on policy match
- ○ Defer delivery of message larger than 0 KB
- ○ Maximum number of attachment 10
- ○ Maximum size message 10240 KB

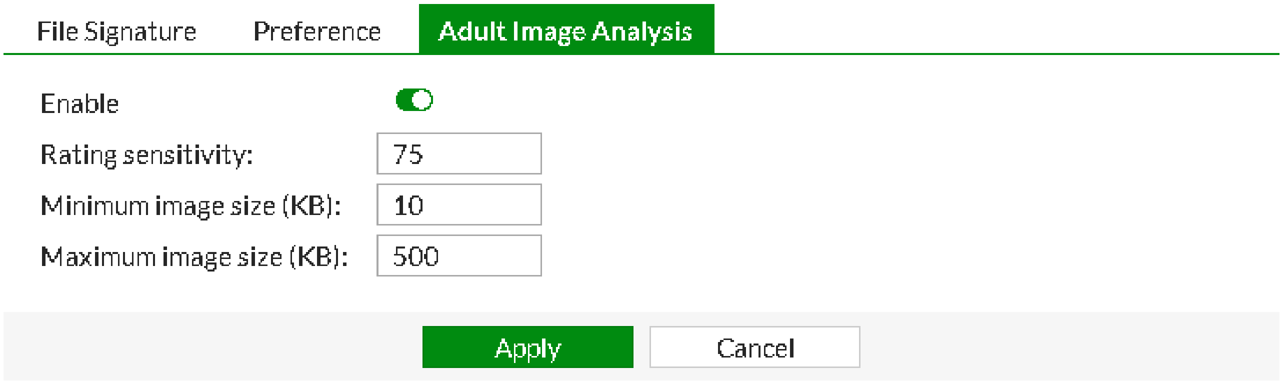
  Action: --Default--
- ● Adult image analysis

  Action: --Default--

Establishing adult image analysis

With the content profile properly configured, we can now move on to configuring adult image analysis settings.

1. Go to **Security > Other > Adult Image Analysis** and click **Enable**.
2. Adjust the **Rating sensitivity** to an appropriate number in order to avoid false-positives and false-negatives. The higher the number, the higher the sensitivity.
3. Enter the **Minimum image size** and **Maximum image size** in kilobytes.
4. Click **Apply**.



Enable: ●

Rating sensitivity: 75

Minimum image size (KB): 10

Maximum image size (KB): 500

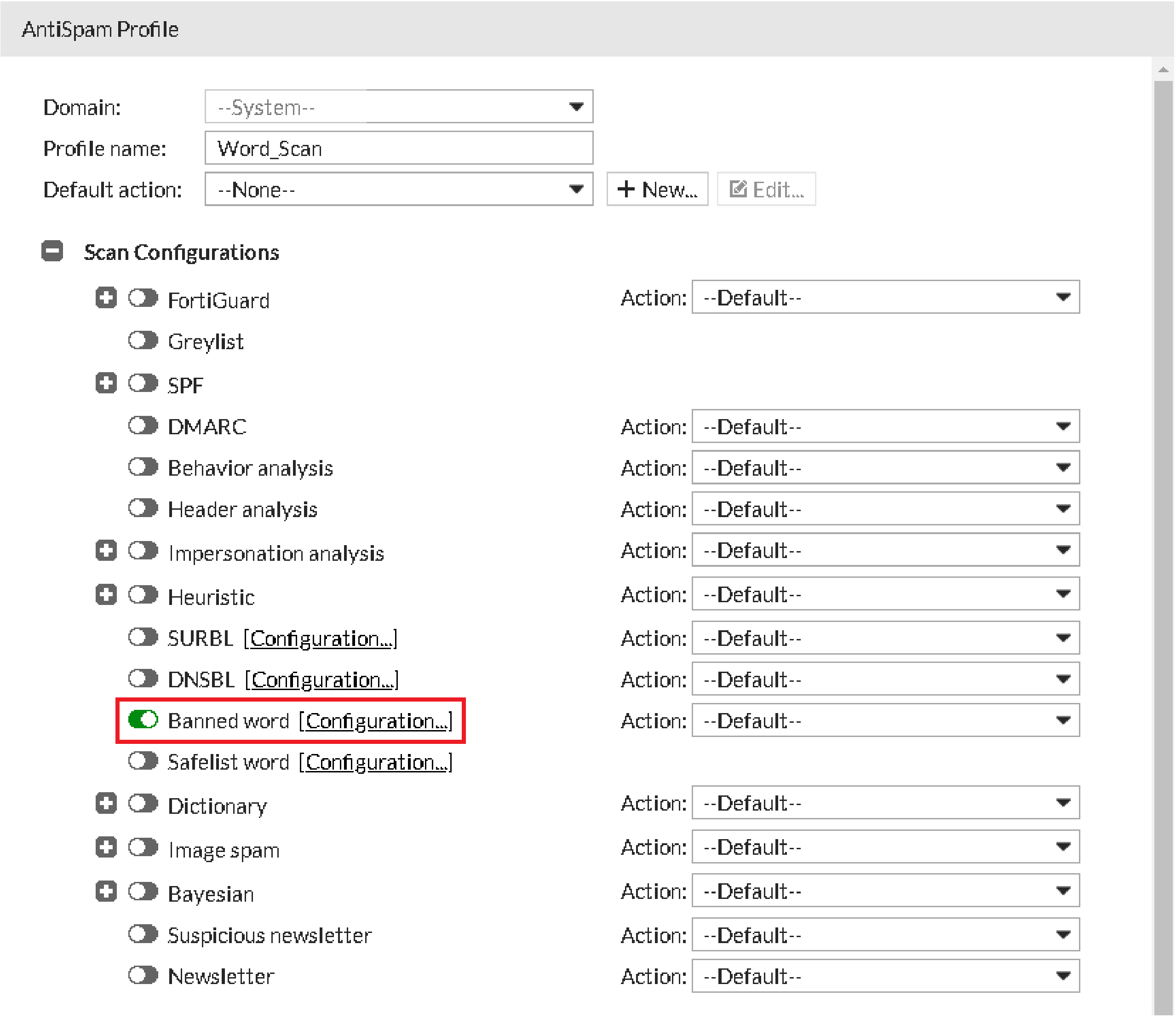
Configuring banned words in FortiMail

What if you know through experience that the occurrence of a certain word in your emails is typically linked to spam? FortiMail can scan an email and look for certain banned words and log those messages as spam when the word is detected.

The following recipe guides you through the easy process of configuring your FortiMail unit to scan for banned words and define known safe words that will bypass the scanning process.

Configuring banned word options in an AntiSpam Profile

1. Go to **Profile > AntiSpam > AntiSpam** and click **New**, or edit an existing profile.
2. Enter a **Profile name**.
3. Under **Scan Configurations**, enable **Banned word** and click **Configuration**.



AntiSpam Profile

Domain: --System--

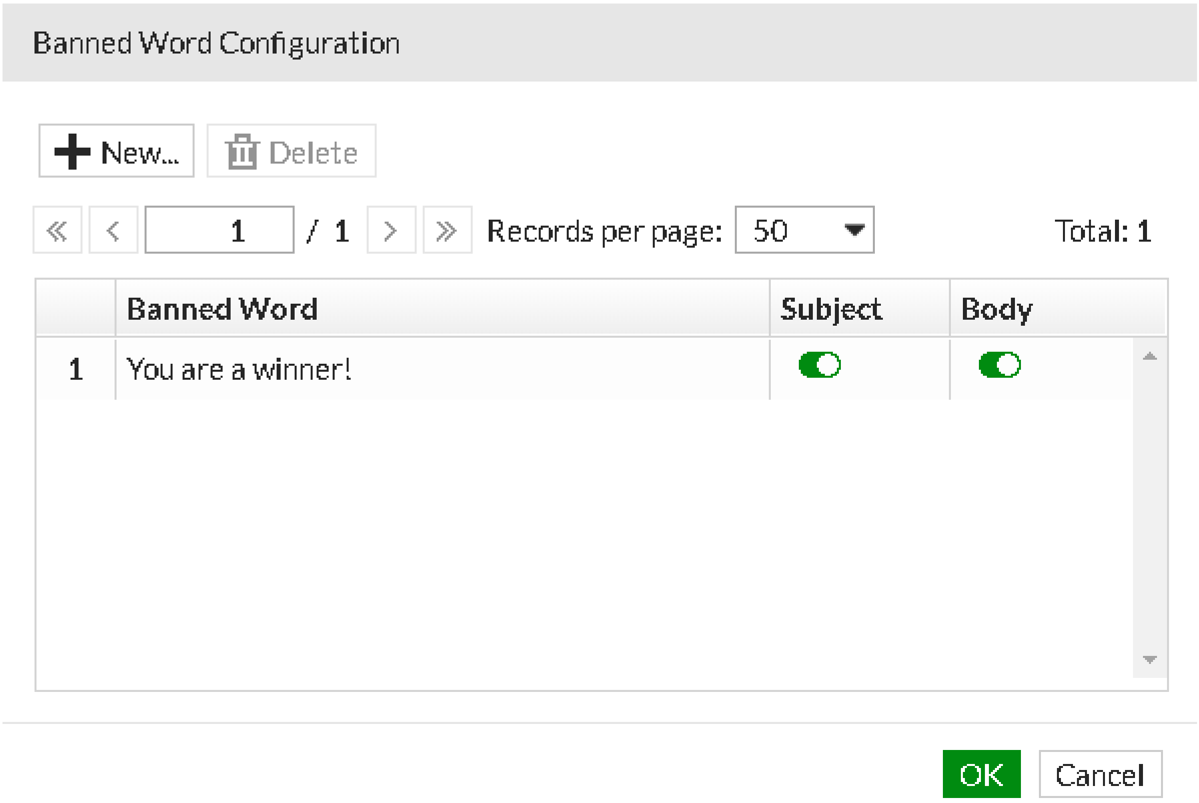
Profile name: Word_Scan

Default action: --None--

Scan Configurations

○ FortiGuard	Action: --Default--
○ Greylist	
○ SPF	
○ DMARC	Action: --Default--
○ Behavior analysis	Action: --Default--
○ Header analysis	Action: --Default--
○ Impersonation analysis	Action: --Default--
○ Heuristic	Action: --Default--
○ SURBL [Configuration...]	Action: --Default--
○ DNSBL [Configuration...]	Action: --Default--
● Banned word [Configuration...]	Action: --Default--
○ Safelist word [Configuration...]	
○ Dictionary	Action: --Default--
○ Image spam	Action: --Default--
○ Bayesian	Action: --Default--
○ Suspicious newsletter	Action: --Default--
○ Newsletter	Action: --Default--

4. In the **Banned Word Configuration** window, click **New**.
5. Enter the word/s you wish to be banned in the **Banned Word** field.
6. Enable both **Subject** and **Body** to let FortiMail scan both the subject line and body of the email for the banned word.
7. Click **OK**.



Banned Word Configuration

Records per page: 50

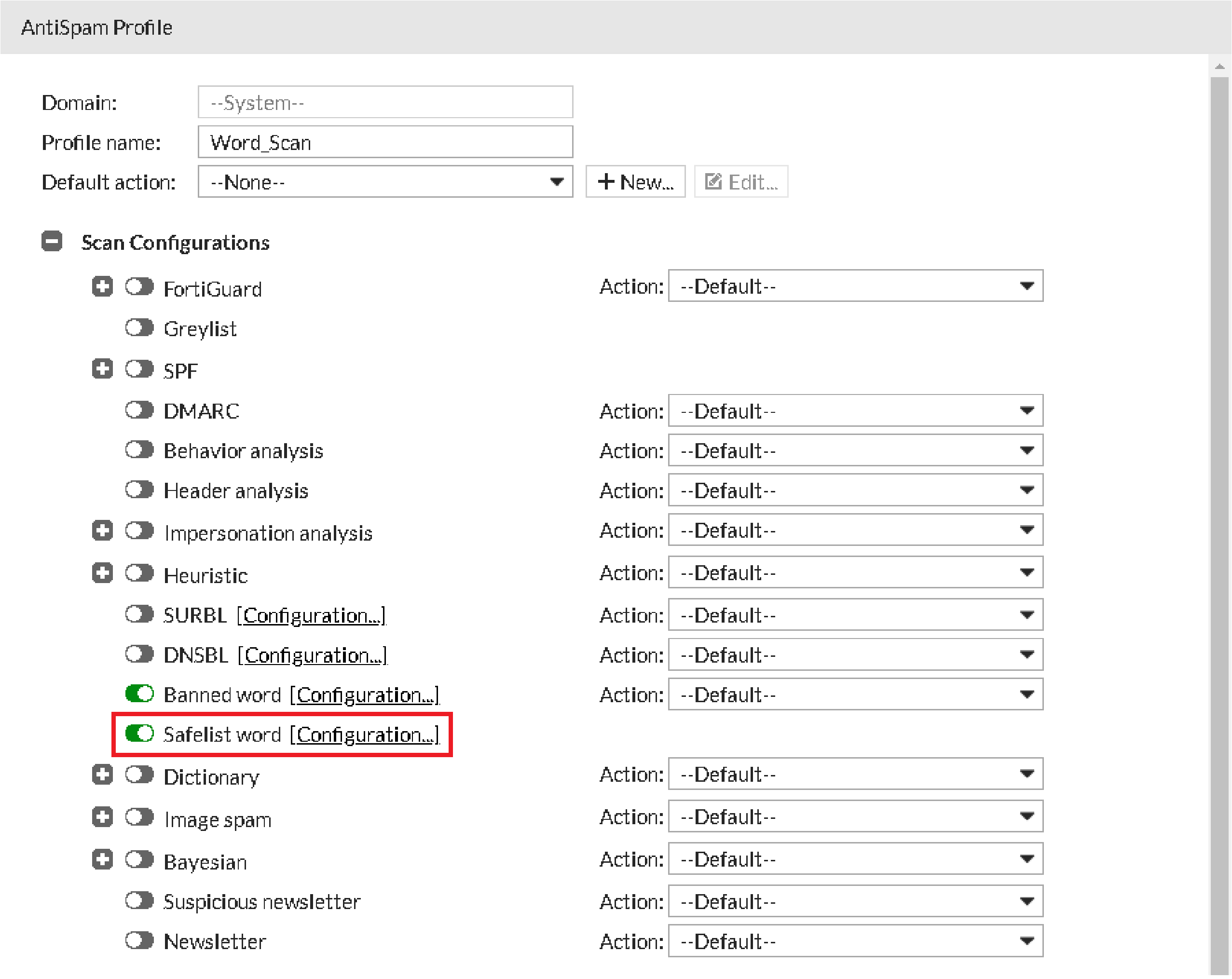
Total: 1

	Banned Word	Subject	Body
1	You are a winner!	✓	✓

Configuring safelist word options

In addition to using banned words to create a blocklist, you can also configure a safelist word section in your profile that tells your FortiMail unit to allow messages whose subject or body contains a particular word. So, for example, FortiMail could be configured to let every email containing the word “meeting” through without scanning.

1. Go to **Profile > AntiSpam > AntiSpam** and edit the same profile from the previous step.
2. Under **Scan Configurations**, enable **Safelist word** and click **Configuration**.



AntiSpam Profile

Domain: --System--

Profile name: Word_Scan

Default action: --None--

Scan Configurations

○ FortiGuard	Action: --Default--
○ Greylist	
○ SPF	
○ DMARC	Action: --Default--
○ Behavior analysis	Action: --Default--
○ Header analysis	Action: --Default--
○ Impersonation analysis	Action: --Default--
○ Heuristic	Action: --Default--
○ SURBL [Configuration...]	Action: --Default--
○ DNSBL [Configuration...]	Action: --Default--
● Banned word [Configuration...]	Action: --Default--
● Safelist word [Configuration...]	
○ Dictionary	Action: --Default--
○ Image spam	Action: --Default--
○ Bayesian	Action: --Default--
○ Suspicious newsletter	Action: --Default--
○ Newsletter	Action: --Default--

3. In the **Safe List Configuration** window, click **New**.
4. Enter the word/s you wish to bypass scanning in the **Safelist Word** field.
5. Enable both **Subject** and **Body** to let FortiMail scan both the subject line and body of the email.
6. Click **OK**.

Blocking the email of a known threat

What if a user on your network has recently downloaded a virus onto their computer and they are now sending out emails that contain harmful malware to other people in the office? Until you solve the infection, you need a way to temporarily prevent the infected computer from sending out emails within the network.

Thankfully, FortiMail supports customizable access controls that can automatically reject emails from sources that you know to be infected.

Access control rules, or the access control list (ACL), controls how the FortiMail unit processes email messages. When an SMTP client attempts to deliver email through the FortiMail unit, the FortiMail unit compares each access control rule to the commands used by the SMTP client during the SMTP session. So, if you wanted to prevent a known infected source from sending you email, you would set your FortiMail unit to reject emails from that source.

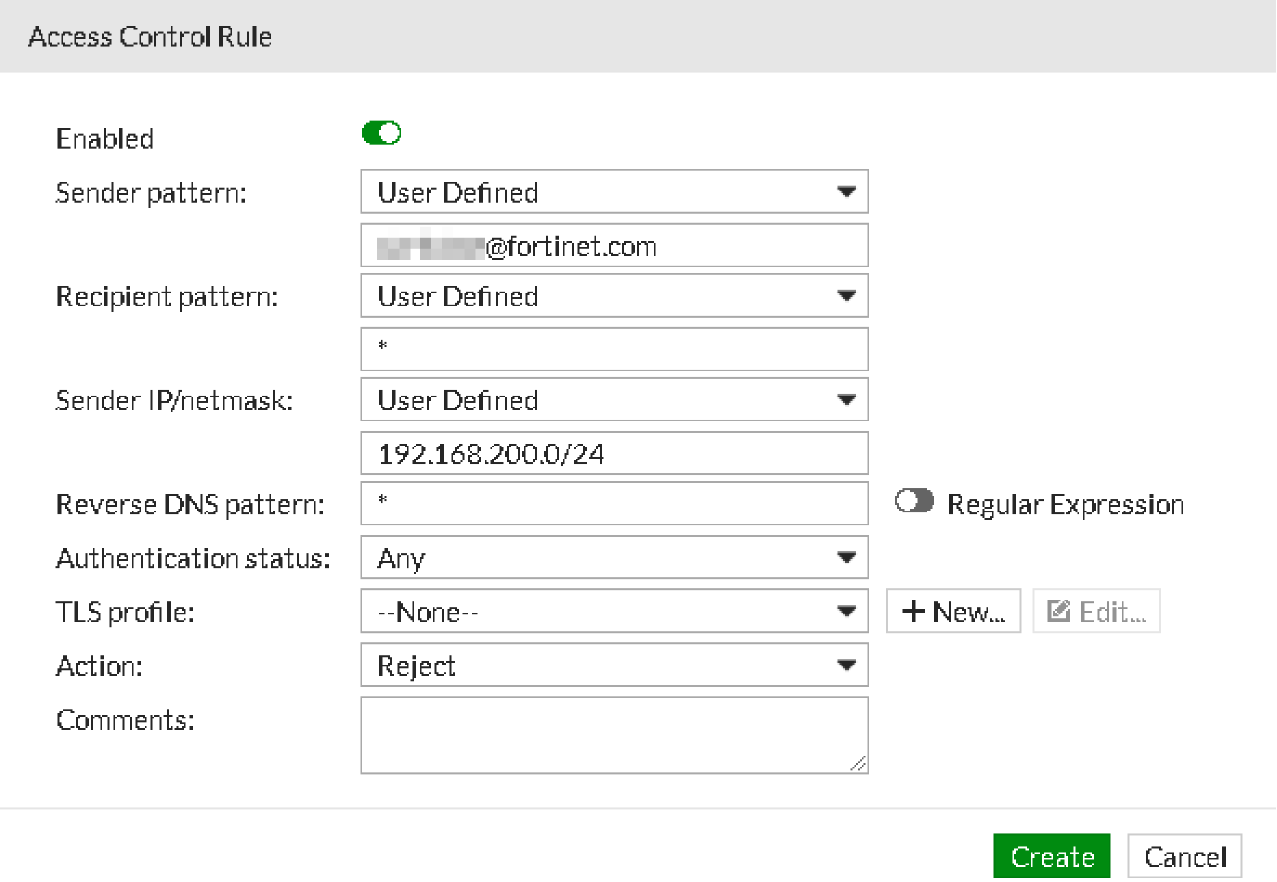
This recipe assumes you have already created an inbound recipient policy.

Configuring access controls

1. Go to **Policy > Access Control > Receiving** and click **New**, or edit an existing access control rule.
2. Click **Enabled**.
3. Set **Sender pattern** to **User Defined**, and enter the user's email address in the field below.
4. Note that it may be preferable to enter the IP address instead of the email address, as it will still allow the user to send and receive emails using their email address from a different machine that is not infected.

   In this case, set **Sender IP/netmask** to **User Defined** also, and enter the user's IP address and netmask.

5. Set **Action** to **Reject**, and click **Create**.



Access Control Rule

Enabled	●
Sender pattern:	User Defined ▾ [redacted]@fortinet.com
Recipient pattern:	User Defined ▾ *
Sender IP/netmask:	User Defined ▾ 192.168.200.0/24
Reverse DNS pattern:	* ○ Regular Expression
Authentication status:	Any ▾
TLS profile:	--None-- ▾ + New... Edit...
Action:	Reject ▾
Comments:	

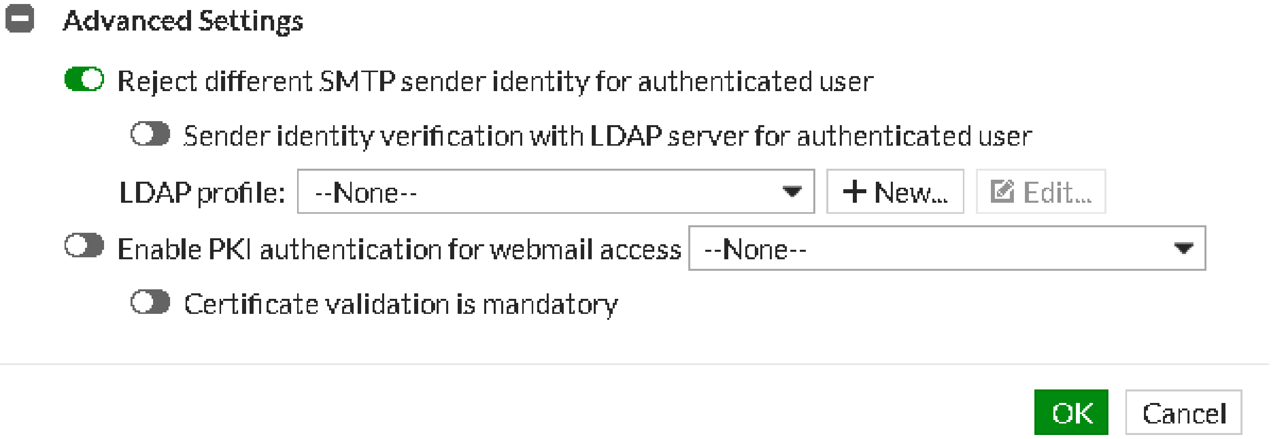
Configuring policies

Since it is possible for an individual to intentionally send an infected email by changing the sender's email address, you must enable **Reject different SMTP sender identify for authenticated user** in the relevant recipient-based policies.

Note that these steps are not necessary if you have already blocked the machine's IP address.

1. Go to **Policy > Recipient Policy > Inbound** and edit your policy.
2. Under **Advanced Settings**, enable **Reject different SMTP sender identity for authenticated user**.

3. Click **OK**.



Advanced Settings

● Reject different SMTP sender identity for authenticated user

○ Sender identity verification with LDAP server for authenticated user

LDAP profile: --None--

○ Enable PKI authentication for webmail access --None--

○ Certificate validation is mandatory

Downloading oversized email attachments

When an email message exceeds the maximum allowed size, it's usually blocked by default. The message size limit settings can be found in the following three places:

- **Content profiles**: Under **Scan Options** when configuring a profile under **Profile > Content > Content**, you can specify both the message size limits and the actions to take.
- **Domain settings**: Under **Advanced Settings > Other** when configuring a profile under **Domain & User > Domain > Domain**, you can also specify the size limit at the domain level. The default size limit is 204800 KB. Messages over this size will be blocked, however this should be a large enough limit for most oversized messages.
- **Session profiles**: Under **SMTP Limits** when configuring a profile under **Profile > Session > Session**, you can specify the message size limits used this session profile. The default size limit is 10240 KB. Messages over this size will be blocked.

However, in some cases, you may not want to block the files. For instance, you may want employees in your organization to send larger files to each other.

In this case, you can use the content profile to catch the email, quarantine the email, and then notify the recipient to download the email attachments from their personal quarantines.

The following example shows how to send and download oversized email messages.

Configuring MS Exchange

This example assumes that you use MS Exchange Server 2010 as your mail server.

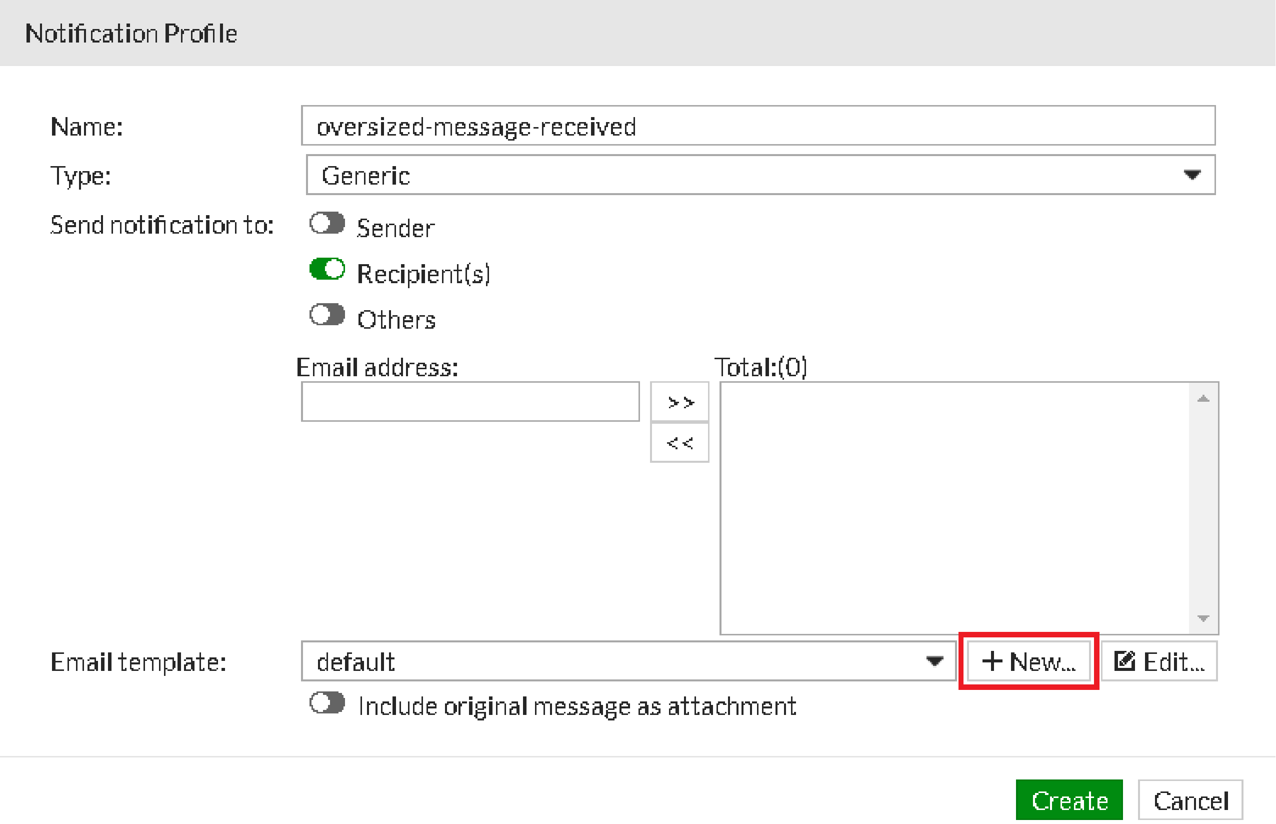
First you need to configure the mail server to allow messages up to 25 MB, for example.

1. In the Exchange Management Console (EMC), go to **mail flow > receive connectors**.
2. Select your transport hub and click **Edit**.
3. Make sure the **Maximum receive message size (MB)** is set to at least **25** and then click **save**.
4. Go to **mail flow > send connectors**.
5. Select the appropriate connector and click **Edit**.
6. Make sure the **Maximum send message size (MB)** is set to at least **25** and then click **save**.
7. Double-click **Outbound Internet Email**.
8. Set **Maximum message size** to **25000**.
9. Go to **Recipients > Mailboxes**.
10. Select your user mailbox and click **Edit**.
11. Under **Mailbox properties**, click **Mailbox Features**.
12. Under **Message Size Restrictions**, click **View details**.
13. Enter **25000** for both the sent and received message fields.
14. Click **OK** and **Save** to confirm the changes.

Configuring notification profiles

Now you need to configure FortiMail to send a notification message instructing the recipient where to obtain the file from quarantine.

1. Go to **Profile > Notification > Notification** and click **New** to create a notification and name it **oversized-message-received**.
2. Set **Type** to **Generic** and enable **Recipient(s)**.
3. Click **New** to create a new email template.



Notification Profile

Name: oversized-message-received

Type: Generic

Send notification to: ○ Sender ● Recipient(s) ○ Others

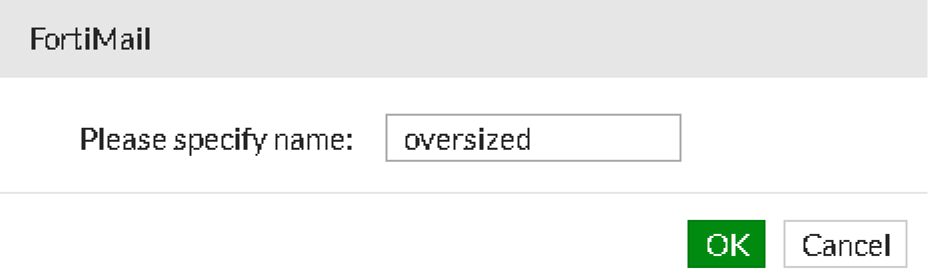
Email address:

Total:(0)

Email template: default

○ Include original message as attachment

4. Name the template **oversized** and click **OK**.



FortiMail

Please specify name: oversized

5. Click **Edit** to modify the newly created template.
6. Fill the email template by copying and pasting the following text and entering it in the following fields:

   Subject: Oversized Message from %%ORIG_ENVELOPE_FROM%% has been sent to quarantine

   From: %%NOTIFY_FROM%%

To: %%NOTIFY_TO%%

Envelope from: %%NOTIFY_FROM%%

Envelope to: %%ORIG_ENVELOPE_TO%%

Content > HTML:

You have received an email that exceeds the 25 MB file size limitation. The file has been routed to your quarantine mailbox.

If you recognize the sender of this message, visit your quarantine mailbox to open the message and download the attachment.

Do not release the message, since it will be rejected at the internal mail server.

If you do not see the message in your quarantine, select the UNRELEASED popup in the upper right corner and change it to RELEASED.

MESSAGE DETAILS

To: %%ORIG_TO%%

From: %%ORIG_FROM%%

Subject: %%ORIG_SUBJECT%%

Time: %%ORIG_DATE%%

Content > Text:

You have received an email that exceeds the 25 MB file size limitations. The file has been routed to your quarantine mailbox.

If you recognize the sender of this message, visit your quarantine mailbox to open the message and download the attachment: https://myfortimail.mycompany.com/m/webmail/Webmail.html#/mailbox/Bulk

Do not release the message, since it will be rejected at the internal mail server.

If you do not see the message in your quarantine, select the UNRELEASED popup in the upper right corner and change it to RELEASED.

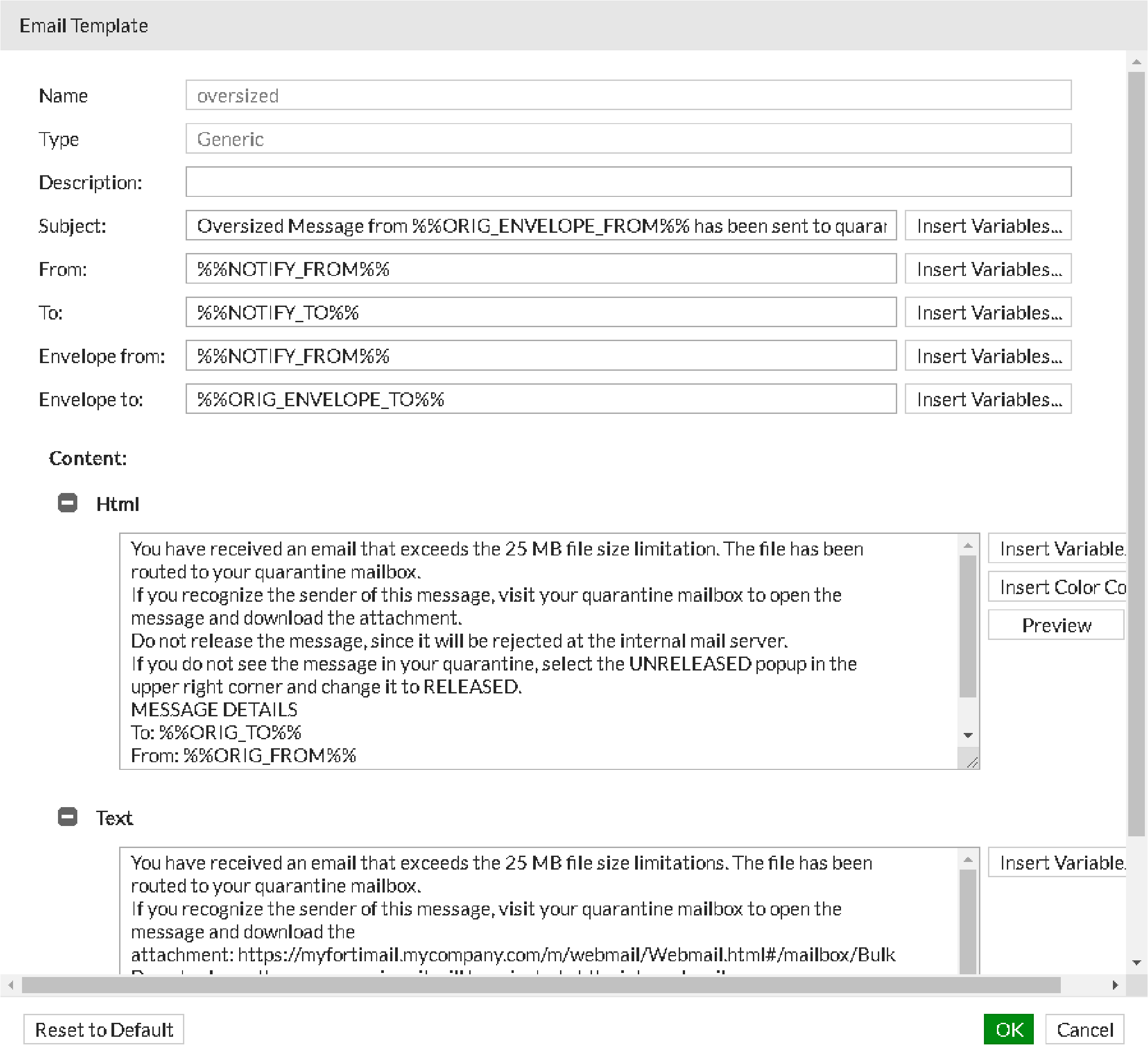
MESSAGE DETAILS

——————————————————————-

To:%%ORIG_TO%%

From:%%ORIG_FROM%%

Subject: %%ORIG_SUBJECT%%



Email Template

Name: oversized

Type: Generic

Description:

Subject: Oversized Message from %%ORIG_ENVELOPE_FROM%% has been sent to quarar

From: %%NOTIFY_FROM%%

To: %%NOTIFY_TO%%

Envelope from: %%NOTIFY_FROM%%

Envelope to: %%ORIG_ENVELOPE_TO%%

Content:

Html

You have received an email that exceeds the 25 MB file size limitation. The file has been routed to your quarantine mailbox.
If you recognize the sender of this message, visit your quarantine mailbox to open the message and download the attachment.
Do not release the message, since it will be rejected at the internal mail server.
If you do not see the message in your quarantine, select the UNRELEASED popup in the upper right corner and change it to RELEASED.
MESSAGE DETAILS
To: %%ORIG_TO%%
From: %%ORIG_FROM%%

Text

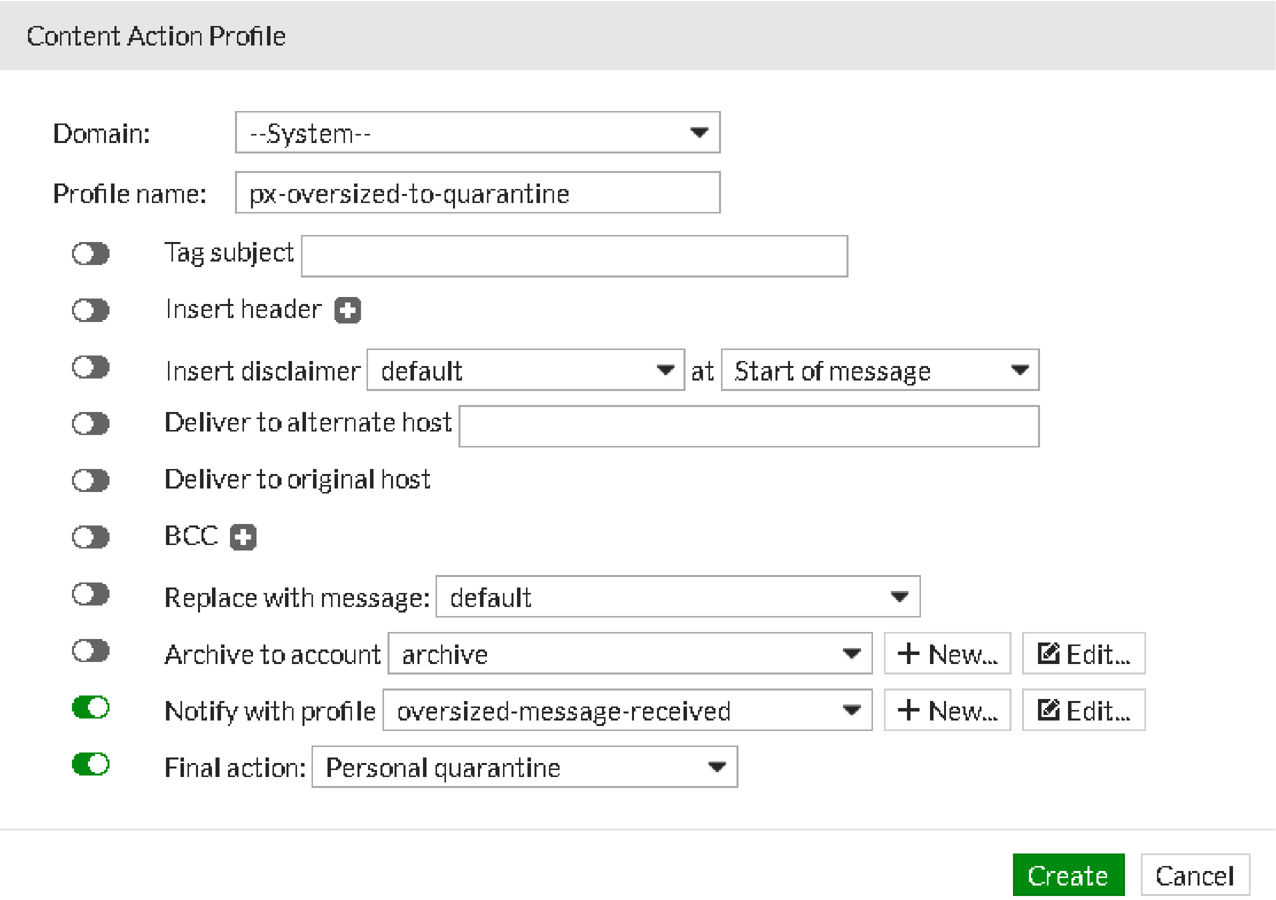
You have received an email that exceeds the 25 MB file size limitations. The file has been routed to your quarantine mailbox.
If you recognize the sender of this message, visit your quarantine mailbox to open the message and download the attachment: https://myfortimail.mycompany.com/m/webmail/Webmail.html#/mailbox/Bulk

7. Click **OK** and then **Create**.

Configuring content profiles and recipient profiles

Now you'll need to create a content profile to use the notification action, and an inbound recipient policy to use the content profile.

1. Go to **Profile > Content > Action** and click **New**.
2. Enter a **Profile name** (in the example, **px-oversized-to-quarantine**).
3. Enable **Notify with profile** and select the **oversized-message-received** profile created earlier from the drop-down menu.
4. Enable **Final action** and select **Personal quarantine** from the drop-down menu.
5. Click **Create**.



Content Action Profile

Domain: --System--

Profile name: px-oversized-to-quarantine

○ Tag subject

○ Insert header

○ Insert disclaimer default at Start of message

○ Deliver to alternate host

○ Deliver to original host

○ BCC

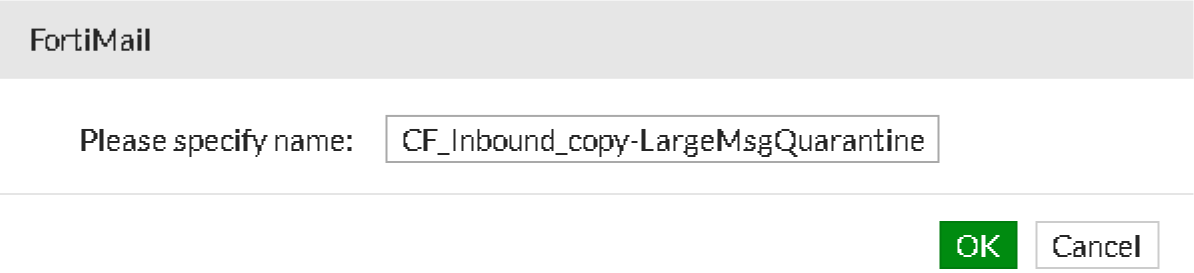
○ Replace with message: default

○ Archive to account archive

● Notify with profile oversized-message-received

● Final action: Personal quarantine

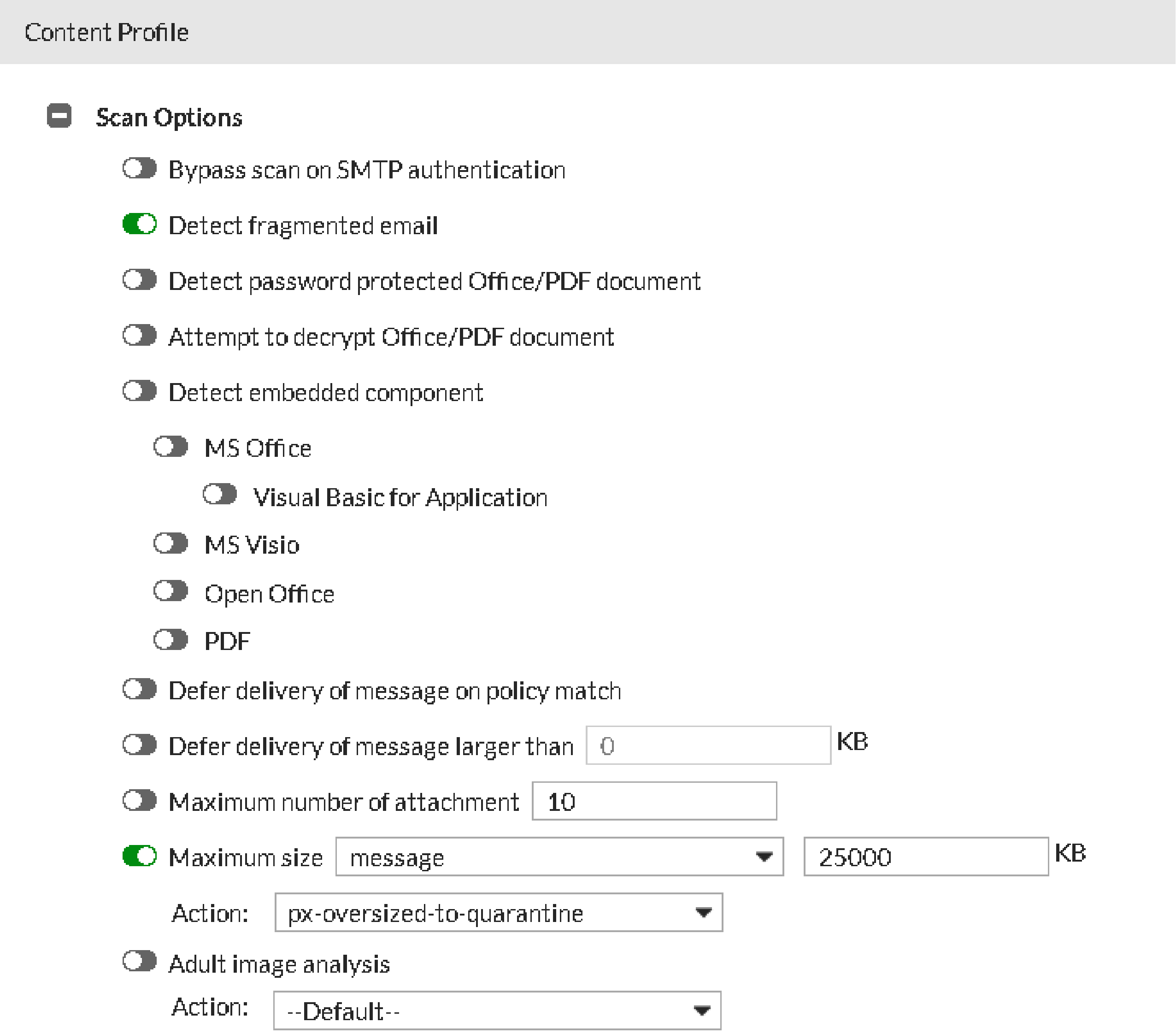
6. Go to **Profile > Content > Content**. Select the content profiles that are referenced in active content policies (these can be viewed under **Policy > Recipient Policy > Inbound**) and click **Clone**.
7. Provide the policy the same name but add **-LargeMsgQuarantine** at the end, as shown in the example below.



FortiMail

Please specify name: CF_Inbound_copy-LargeMsgQuarantine

8. Select the newly created clone and click **Edit**.
9. Expand **Scan Options**. Enable and set the maximum message size to **25000**, and set the **Action** to **px-oversized-to-quarantine**.



Content Profile

Scan Options

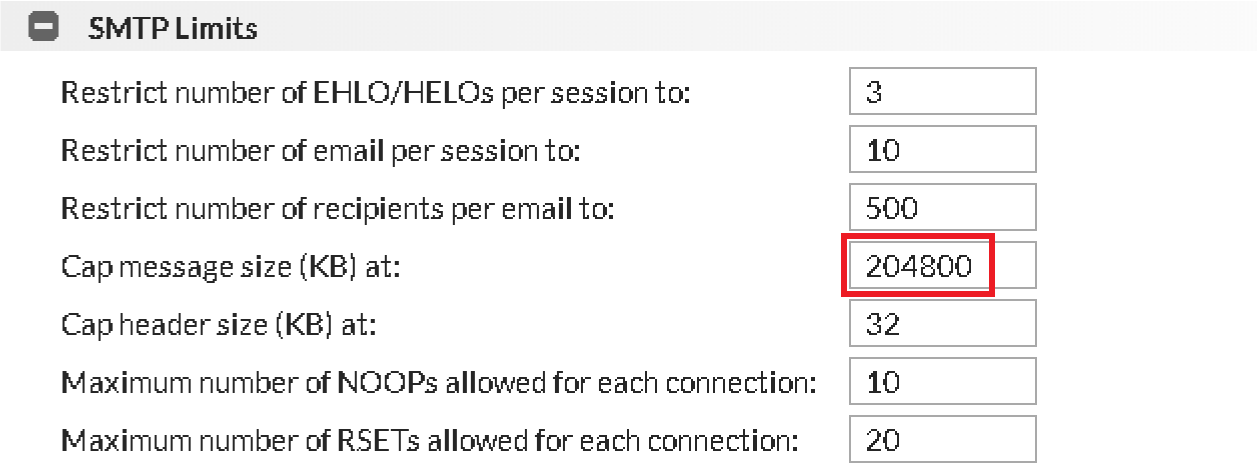
- ○ Bypass scan on SMTP authentication
- ● Detect fragmented email
- ○ Detect password protected Office/PDF document
- ○ Attempt to decrypt Office/PDF document
- ○ Detect embedded component
  - ○ MS Office
    - ○ Visual Basic for Application
  - ○ MS Visio
  - ○ Open Office
  - ○ PDF
- ○ Defer delivery of message on policy match
- ○ Defer delivery of message larger than 0 KB
- ○ Maximum number of attachment 10
- ● Maximum size message 25000 KB
  - Action: px-oversized-to-quarantine
- ○ Adult image analysis
  - Action: --Default--

10. Go to **Policy > Recipient Policy > Inbound**.
11. Edit each policy that has a content filter profile and apply the newly cloned **LargeMsgQuarantine** profile.

Increasing size limits in session profiles

As mentioned in the introduction to this recipe, the default size limit for domain settings is approximately 204800 KB (or approximately 200 MB). This is the system maximum limit. However, the default 10240 KB session profile SMTP size limit will not allow oversized messages. This setting can be increased.

1. Go to **Profile > Session > Session**, select the inbound session profile you want and click **Edit**.
2. Expand **SMTP Limits** and enter **204800** in the **Cap message size (KB) at** field.
3. Click **OK**.



SMTP Limits

Restrict number of EHLO/HELOs per session to:	3
Restrict number of email per session to:	10
Restrict number of recipients per email to:	500
Cap message size (KB) at:	204800
Cap header size (KB) at:	32
Maximum number of NOOPs allowed for each connection:	10
Maximum number of RSETs allowed for each connection:	20

Configuring incoming email DMARC checking with SPF and DKIM

In this recipe, you configure Domain-based Message Authentication, Reporting & Conformance (DMARC) to perform incoming email authentication with Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM) checking.

SPF compares the client IP address to the IP address of the authorized senders in the DNS record. If the test fails, the email is treated as spam.

DKIM allows FortiMail to check for DKIM signatures for incoming email with the domain keys for the protected domains. DKIM may also be configured to sign outgoing email, but is outside the scope of this recipe.

This recipe covers how to enable SPF, DKIM, and DMARC checking on FortiMail to check incoming email.

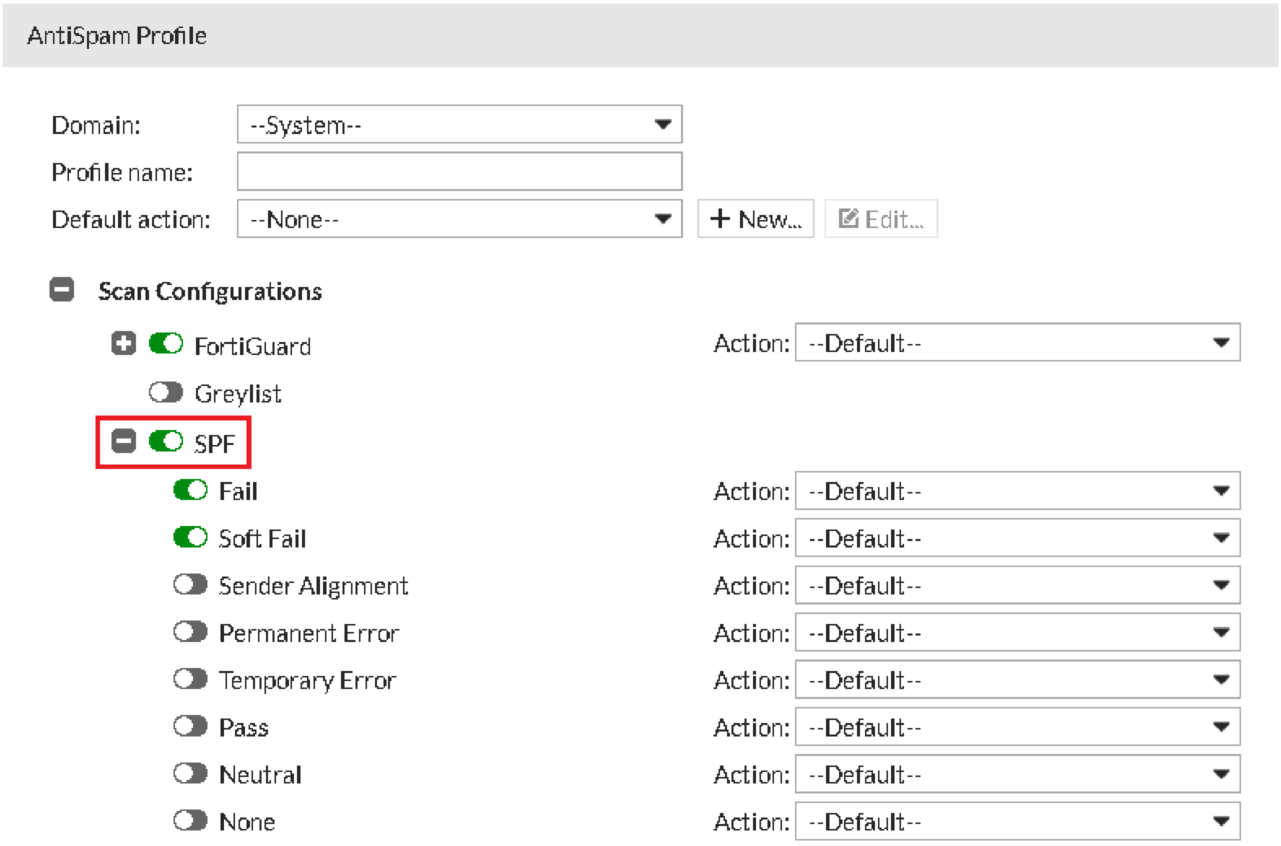
For more information about these email authentication protocols, see the FortiMail Administration Guide.

Enabling SPF checking for incoming email

You can enable SPF in AntiSpam profiles and in session profile settings. Note that if you select **Bypass SPF checking** in a session profile, SPF checking will be bypassed even if it is enabled in an AntiSpam profile.

To enable SPF in an AntiSpam profile:

1. Go to **Profile > AntiSpam > AntiSpam** and click **New**, or edit an existing profile.
2. Under **Scan Configurations**, enable **SPF**. You can also expand **SPF** to have more granular control.



AntiSpam Profile

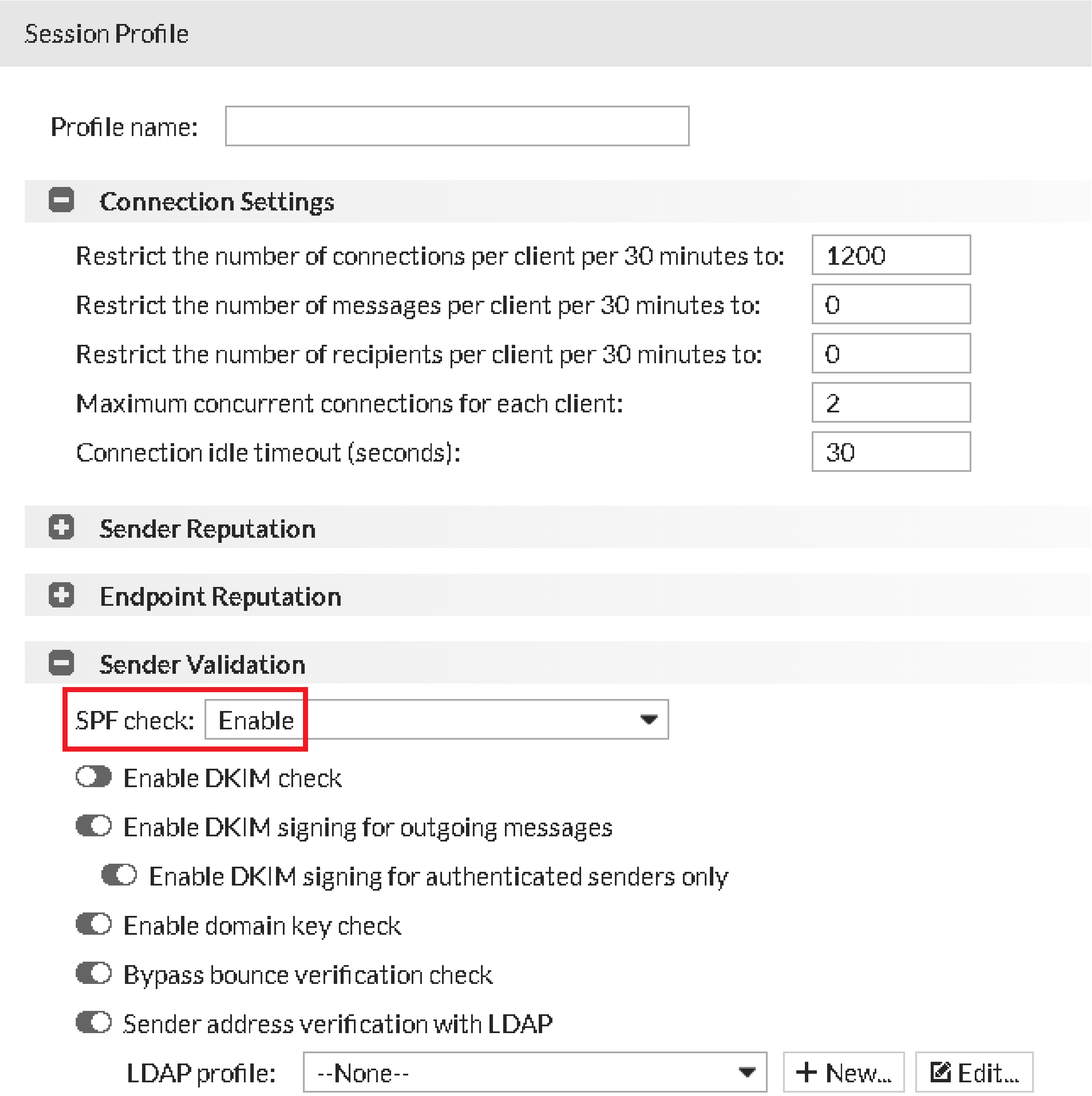
Domain:	--System--
Profile name:	
Default action:	--None--

Scan Configurations

● FortiGuard	Action:	--Default--
○ Greylist		
● SPF		
● Fail	Action:	--Default--
● Soft Fail	Action:	--Default--
○ Sender Alignment	Action:	--Default--
○ Permanent Error	Action:	--Default--
○ Temporary Error	Action:	--Default--
○ Pass	Action:	--Default--
○ Neutral	Action:	--Default--
○ None	Action:	--Default--

To enable SPF in a session profile:

1. Go to **Profile > Session > Session** and click **New**, or edit an existing profile.
2. Under **Sender Validation**, select the appropriate option from the **SPF check** drop-down menu: **Disable**, **Enable**, or **Bypass**.



Session Profile

Profile name:

Connection Settings

Restrict the number of connections per client per 30 minutes to:	1200
Restrict the number of messages per client per 30 minutes to:	0
Restrict the number of recipients per client per 30 minutes to:	0
Maximum concurrent connections for each client:	2
Connection idle timeout (seconds):	30

Sender Reputation

Endpoint Reputation

Sender Validation

SPF check: Enable

Enable DKIM check

Enable DKIM signing for outgoing messages

Enable DKIM signing for authenticated senders only

Enable domain key check

Bypass bounce verification check

Sender address verification with LDAP

LDAP profile: --None--

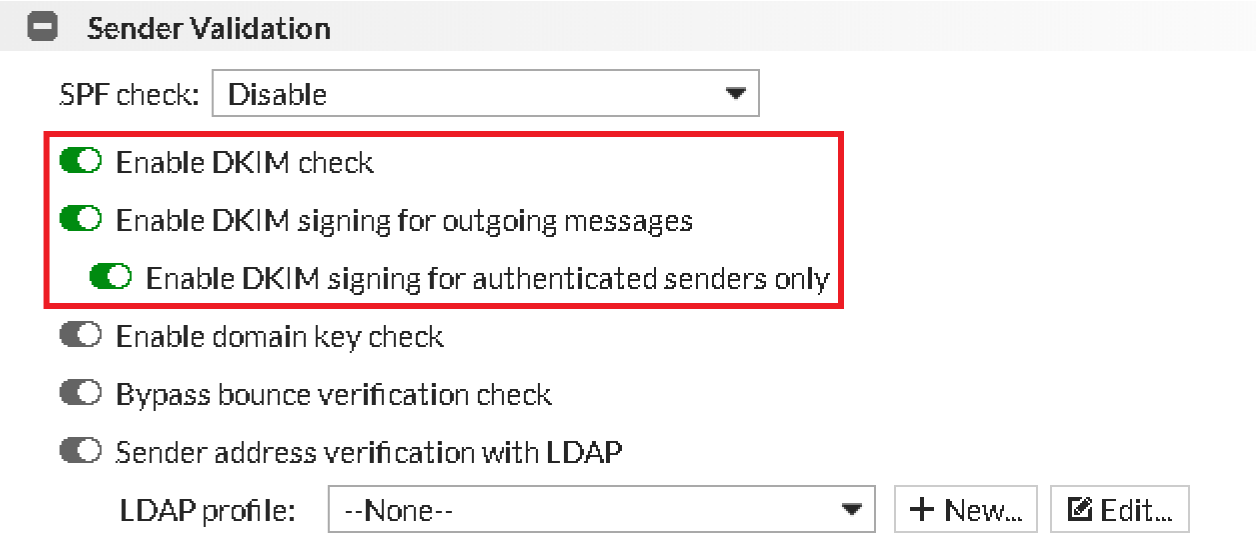
If the sender domain DNS record lists SPF authorized IP addresses, use SPF check to compare the client IP address to the IP addresses of authorized senders in the DNS record. An unauthorized client IP address increases the client sender reputation score, while an authorized client IP address decreases the client sender reputation score.

Enabling DKIM checking for incoming email

FortiMail can perform DKIM checking for the incoming mail by querying the DNS server that hosts the DNS record for the sender's domain name to retrieve its public key to decrypt and verify the DKIM signature.

To enable DKIM checking:

1. Go to **Profile > Session > Session** and click **New**, or edit an existing profile.
2. Under **Sender Validation**, enable the DKIM checking option. DKIM signing options are also available.



Sender Validation

SPF check: Disable

Enable DKIM check

Enable DKIM signing for outgoing messages

Enable DKIM signing for authenticated senders only

Enable domain key check

Bypass bounce verification check

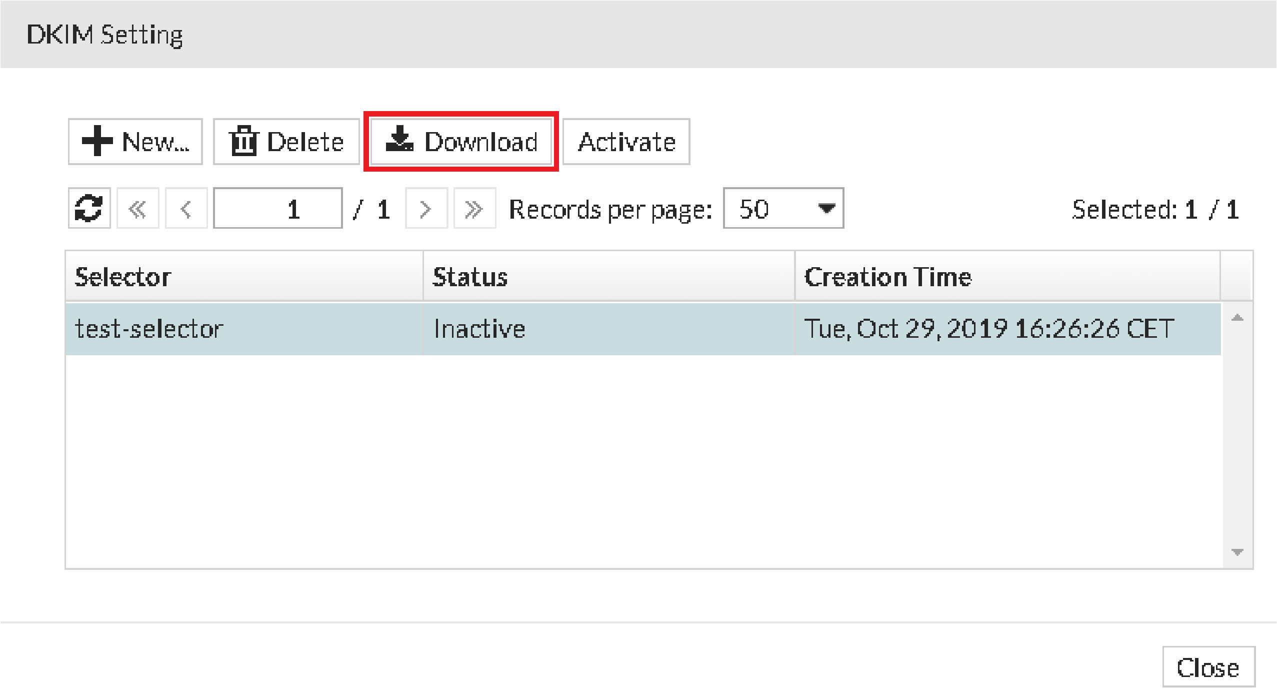
Sender address verification with LDAP

LDAP profile: --None--

To configure DKIM signing:

If you want to sign the outgoing mail with DKIM signatures so that the remote receiving server can verify the signatures, you can do so after you create the protected domains. Note that the DKIM signing settings only appear when configuring an existing protected domain.

1. Go to **Domain & User > Domain > Domain** and click **New**, or edit an existing profile.
2. Under **Advanced Setting**, click **DKIM Setting**.
3. Click **New**.
4. Enter a name in the **New selector** field.
5. Set **DKIM key** to **Auto Generation**. The key pair will be automatically generated and the public key exported for publication on a DNS server.
6. Click **OK**.
7. The new selector will appear. Select the newly created selector and click **Download** to download the domain key DKIM file.



1 / 1 Records per page: 50 Selected: 1 / 1

Selector	Status	Creation Time
test-selector	Inactive	Tue, Oct 29, 2019 16:26:26 CET

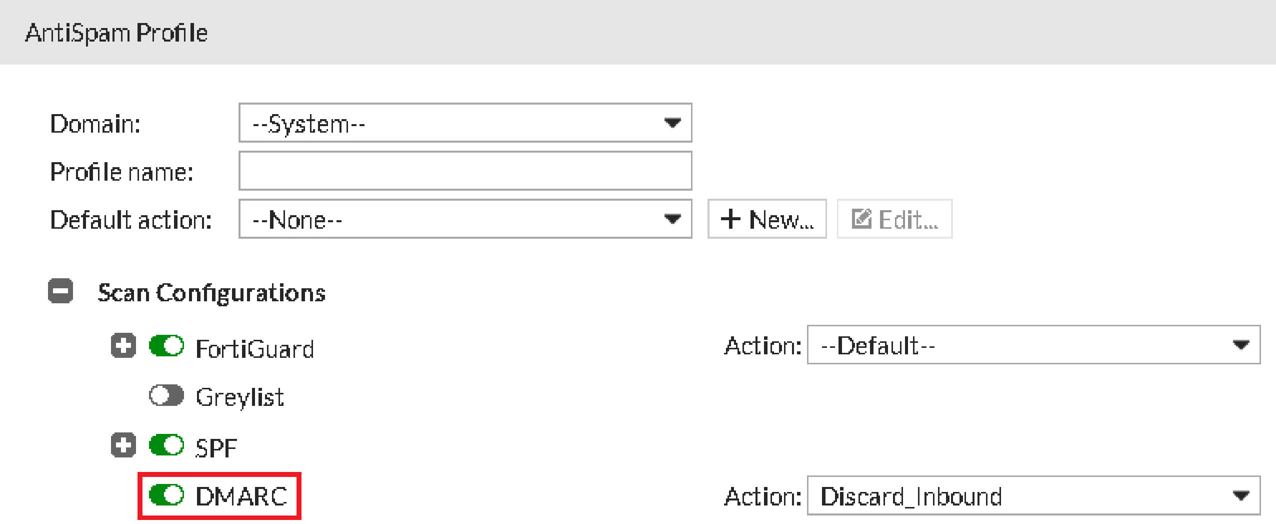
8. Publish the public key by inserting the exported DNS record into the DNS zone file of the DNS server that resolves this domain name.
9. From the **DKIM Setting** window in FortiMail, select the newly created selector and click **Activate**.
10. Click **Close**, and click **OK**.

Enabling DMARC checking for incoming email

DMARC performs email authentication with, and is contingent on, SPF and DKIM checking. If either SPF or DKIM check passes, DMARC check will pass. If both of them fail, DMARC check will fail.

1. Go to **Profile > AntiSpam > AntiSpam** and click **New**, or edit an existing profile.
2. Under **Scan Configurations**, enable **DMARC** and assign the **Discard_Inbound** action from the drop-down menu.

3. Click **Create** or **OK**.



AntiSpam Profile

Domain: --System--

Profile name:

Default action: --None--

Scan Configurations

- FortiGuard — Action: --Default--
- Greylist
- SPF
- DMARC — Action: Discard_Inbound

FortiGuard AntiSpam service with FortiMail

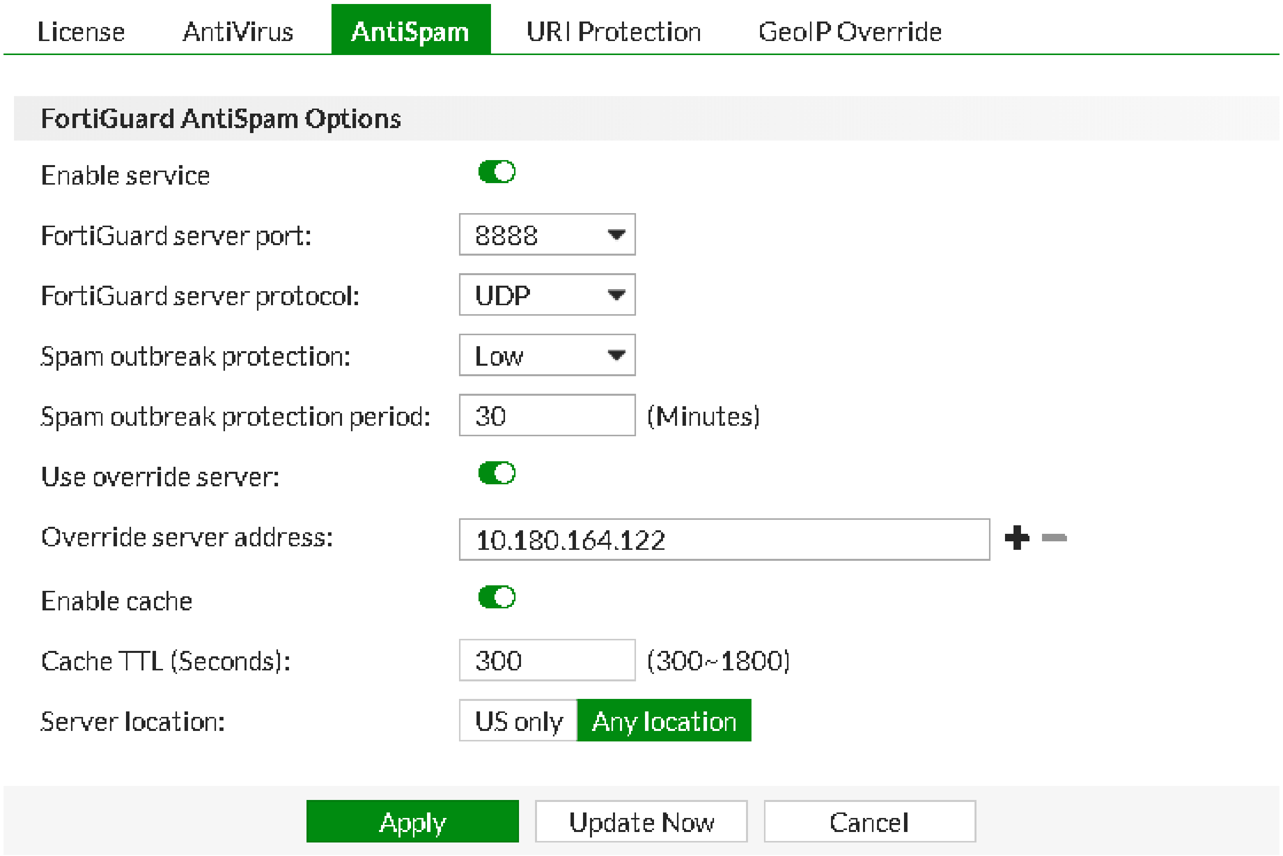
The FortiGuard AntiSpam service uses both a sender IP reputation database and spam signature database to detect and block a wide range of spam messages. FortiGuard AntiSpam is updated regularly to ensure constant protection for your FortiMail system.

This recipe details how FortiGuard AntiSpam operates and guides you through the process of integrating FortiGuard AntiSpam into FortiMail.

Connecting to FortiGuard AntiSpam service

Note that, in order to connect to FortiGuard AntiSpam services, you must have a service contract.

1. Go to **System > FortiGuard > AntiSpam** in the **Advanced Mode** of the FortiMail UI.
2. Click **Enable service**.
3. Optionally, if you have a local server that can provide a faster connection, enter its IP address in the **Override server address** field.
4. Select **Enable cache** and enter a cache time to live (TTL) in seconds in the field provided.
5. Select **Apply**.



FortiGuard AntiSpam Options

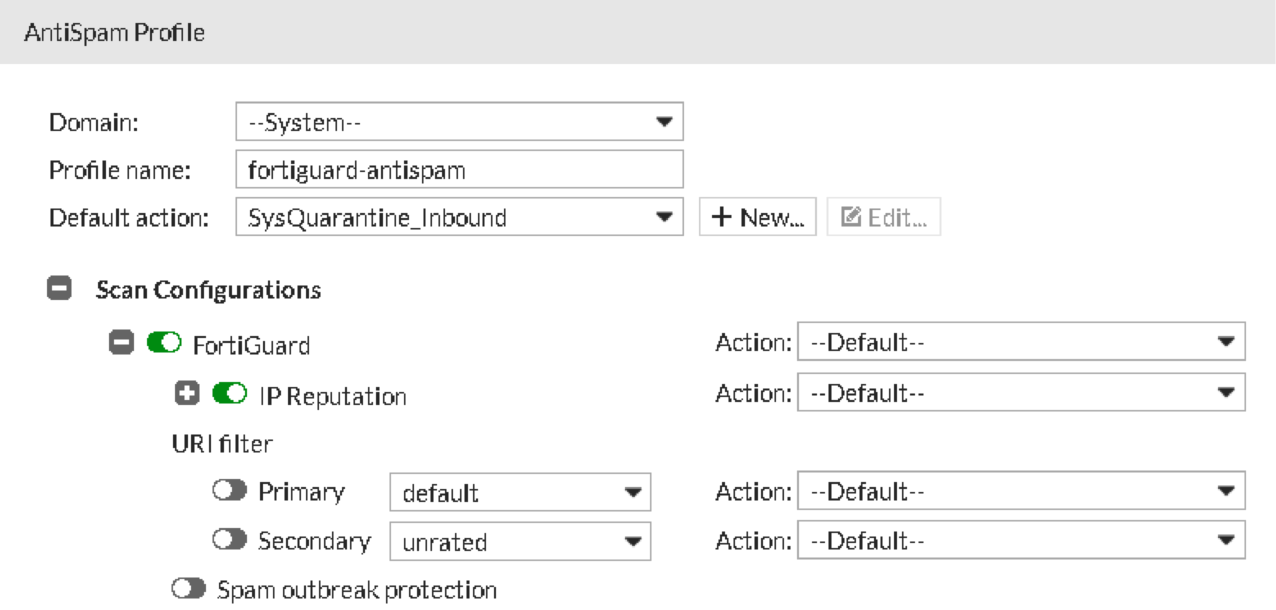
Enable service	●
FortiGuard server port:	8888
FortiGuard server protocol:	UDP
Spam outbreak protection:	Low
Spam outbreak protection period:	30 (Minutes)
Use override server:	●
Override server address:	10.180.164.122
Enable cache	●
Cache TTL (Seconds):	300 (300~1800)
Server location:	US only [✓ Any location]

6. Go to **System > FortiGuard > License**.

7. Expand **FortiGuard AntiSpam Query** and verify the connection by entering an IP address or URL in the **Query input** textbox provided and clicking **Query**.

Creating an AntiSpam profile

1. Go to **Profile > AntiSpam > AntiSpam** and click **New**.
2. Set the profile as either a system-wide or domain-specific profile, and enter a **Profile name**.
3. Set an appropriate **Default action**.
4. Under **Scan Configuration**, enable **FortiGuard**.
5. Click **Create**.



AntiSpam Profile

Domain: --System--

Profile name: fortiguard-antispam

Default action: SysQuarantine_Inbound

Scan Configurations

FortiGuard: enabled — Action: --Default--

IP Reputation: enabled — Action: --Default--

URI filter

Primary: default — Action: --Default--

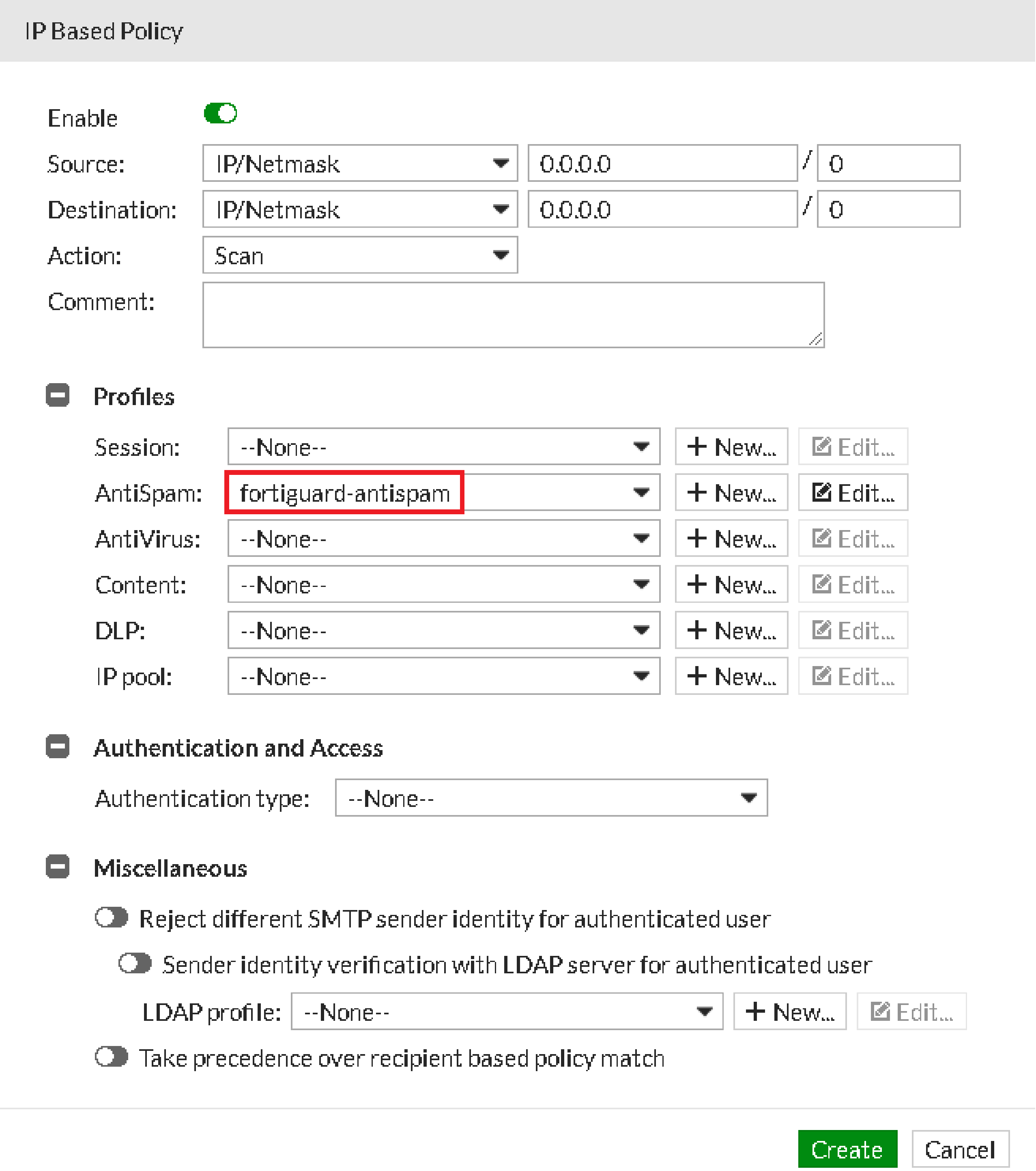
Secondary: unrated — Action: --Default--

Spam outbreak protection

Using the AntiSpam profile in a policy

1. Go to **Policy > IP Policy > IP Policy** and click **New**.
2. Under **Profiles**, select your newly created AntiSpam profile from the **AntiSpam** drop-down menu.

3. Click **Create**.



IP Based Policy

Enable: ●

Source: IP/Netmask 0.0.0.0 / 0

Destination: IP/Netmask 0.0.0.0 / 0

Action: Scan

Comment:

Profiles

Session: --None--

AntiSpam: fortiguard-antispam

AntiVirus: --None--

Content: --None--

DLP: --None--

IP pool: --None--

Authentication and Access

Authentication type: --None--

Miscellaneous

○ Reject different SMTP sender identity for authenticated user

○ Sender identity verification with LDAP server for authenticated user

LDAP profile: --None--

○ Take precedence over recipient based policy match

FortiGuard AntiVirus service with FortiMail

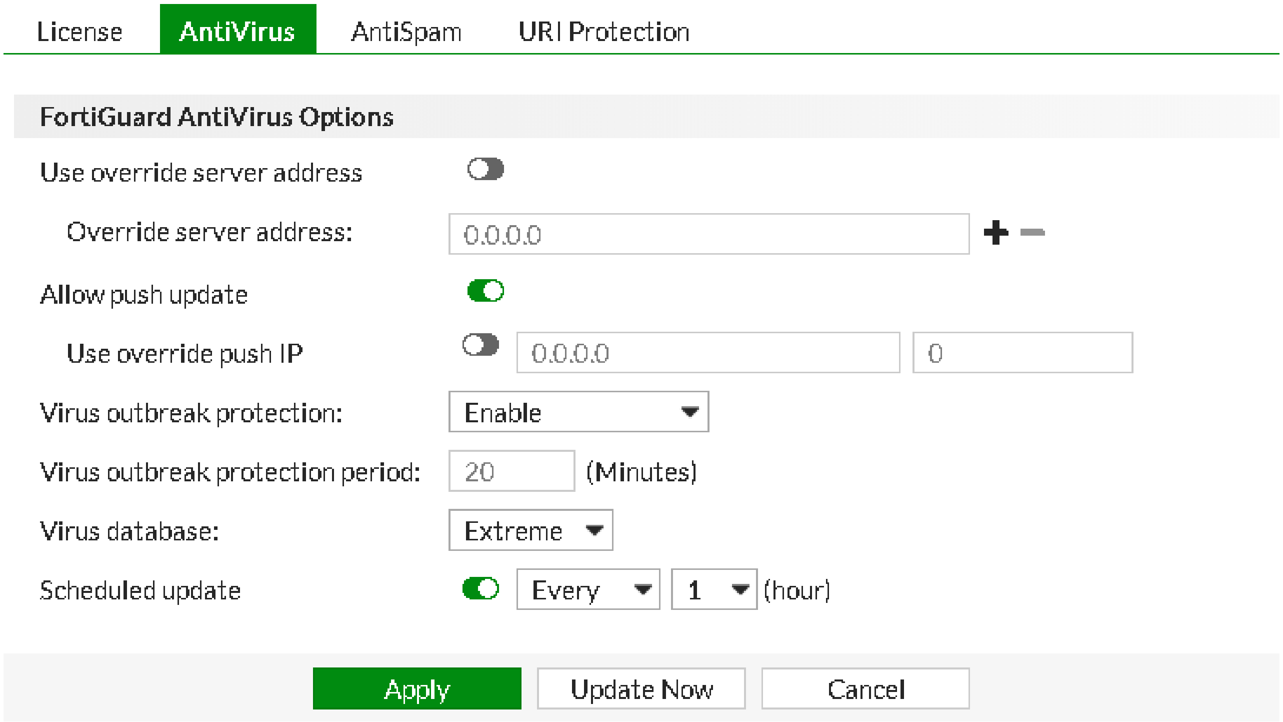
This recipe details how FortiGuard AntiVirus operates and guides you through the process of using FortiGuard AntiVirus.

Using data analytic techniques, FortiGuard labs are able to quickly detect and respond to new outbreaks, blocking Suspicious Virus Objects without the need for antivirus signatures.

Connecting to FortiGuard AntiVirus service

Note that, in order to connect to FortiGuard AntiVirus services, you must have a service contract. To receive the up-to-date antivirus engine and signatures, FortiMail must connect to the FortiGuard server.

1. Go to **System > FortiGuard > AntiVirus** in the **Advanced Mode** of the FortiMail UI.
2. Optionally, if you have a local server that can provide a faster connection, enable **Use override server address** and enter its IP address in the **Override server address** field.
3. Enable **Allow push update** to allow the FortiMail unit to accept push notifications. Push notifications only notify the FortiMail unit that an update is available and do not transmit the update itself.
4. Enable **Scheduled update** and use the drop-down menus to define how often the connection to FortiGuard AntiVirus is updated.
5. Click **Apply**.



FortiGuard AntiVirus Options

Use override server address ○

Override server address: 0.0.0.0 + −

Allow push update ●

Use override push IP ○ 0.0.0.0 0

Virus outbreak protection: Enable

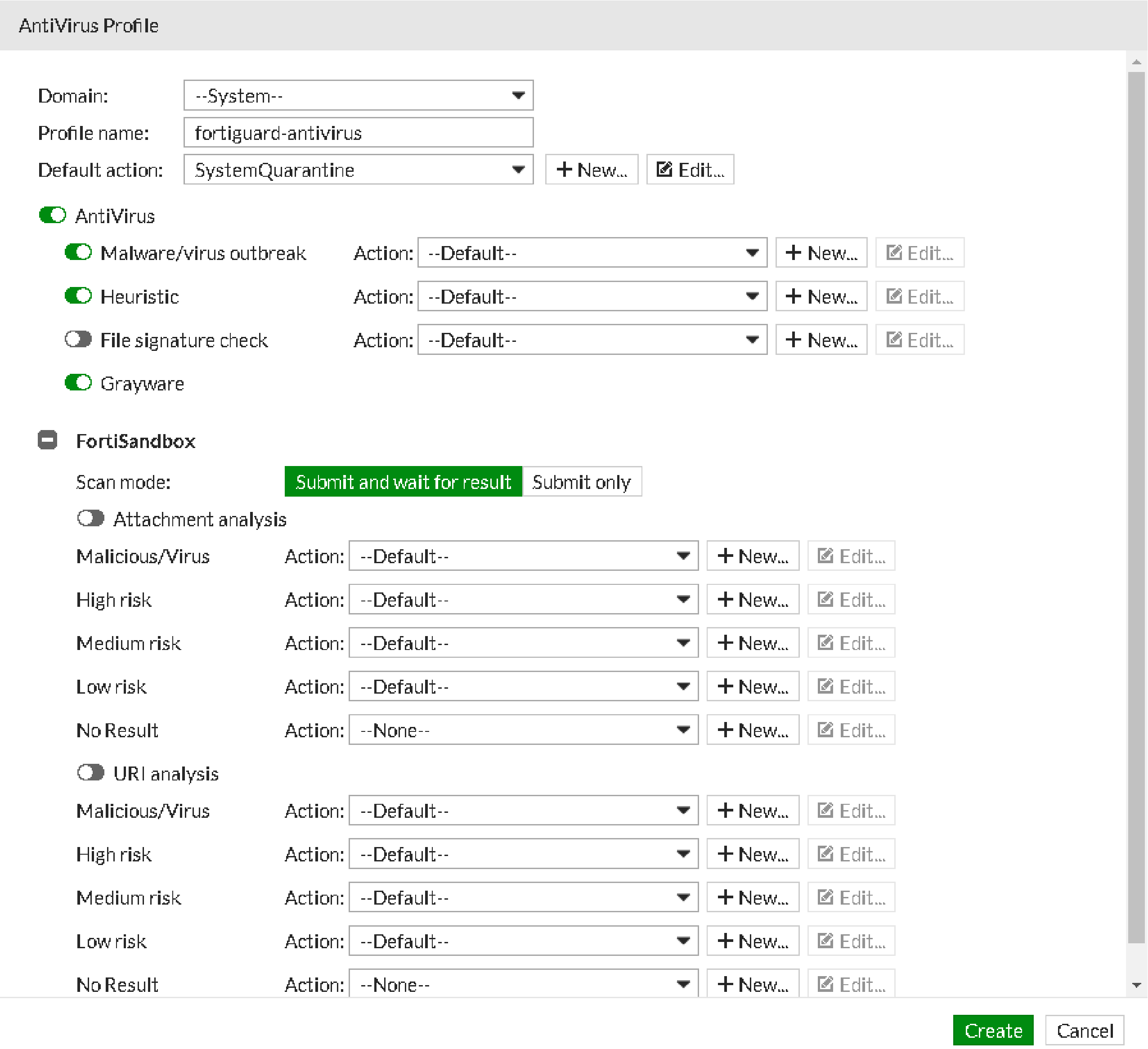
Virus outbreak protection period: 20 (Minutes)

Virus database: Extreme

Scheduled update ● Every 1 (hour)

Creating an AntiVirus profile

1. Go to **Profile > AntiVirus > AntiVirus** and click **New**.
2. Set the profile as either a system-wide or domain-specific profile, and enter a **Profile name**.
3. Set an appropriate **Default action**.
4. Enable **AntiVirus**, and enable and define the appropriate **Action** for the options available.
5. If you have a FortiSandbox, under **FortiSandbox**, define an appropriate **Scan mode** and configure the various options available.
6. Select **Create**.



AntiVirus Profile

Domain: --System--

Profile name: fortiguard-antivirus

Default action: SystemQuarantine

AntiVirus: enabled

Malware/virus outbreak (enabled)	Action: --Default--
Heuristic (enabled)	Action: --Default--
File signature check (disabled)	Action: --Default--
Grayware (enabled)	

FortiSandbox

Scan mode: Submit and wait for result | Submit only

Attachment analysis (disabled)

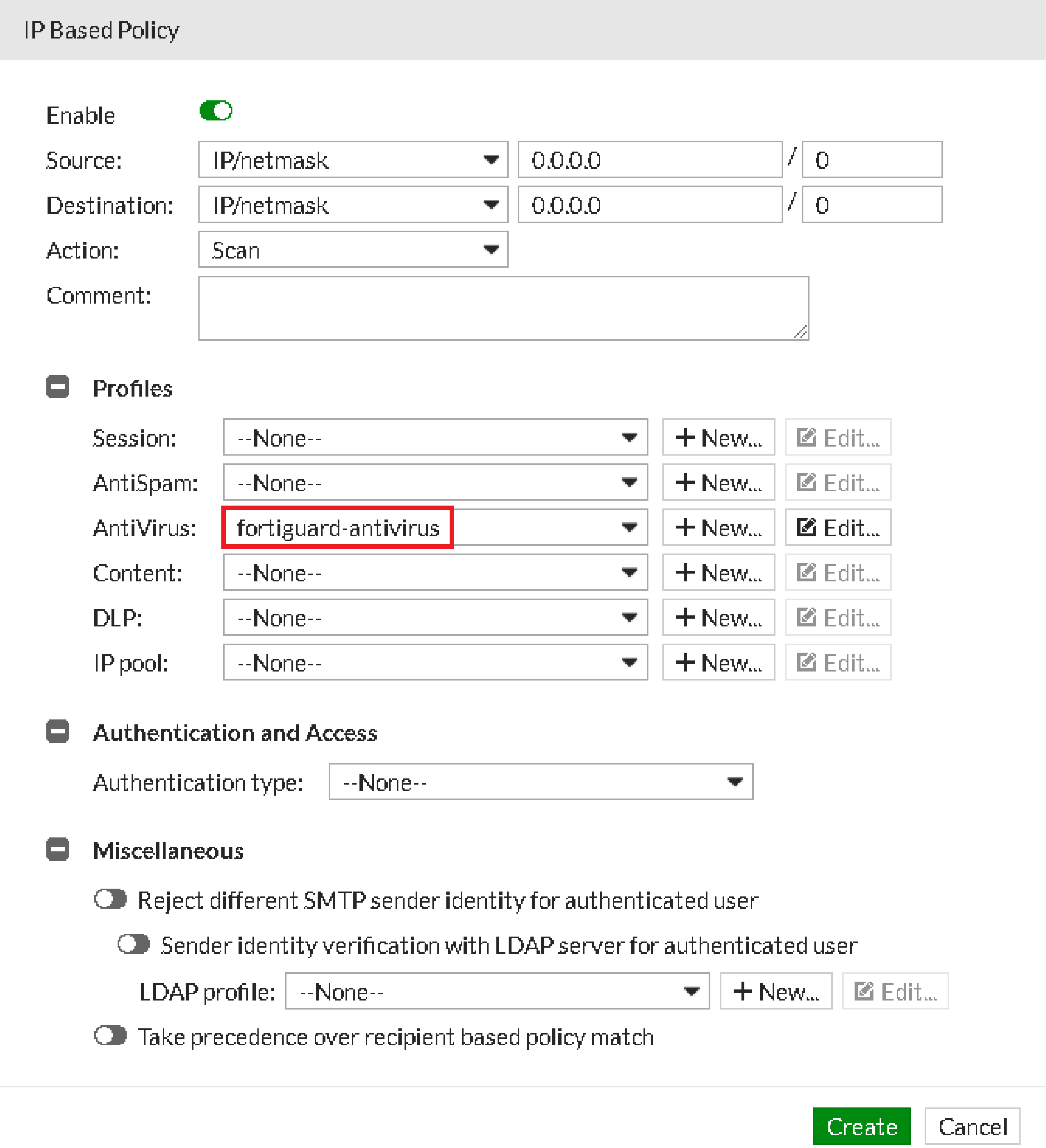
Malicious/Virus	Action: --Default--
High risk	Action: --Default--
Medium risk	Action: --Default--
Low risk	Action: --Default--
No Result	Action: --None--

URI analysis (disabled)

Malicious/Virus	Action: --Default--
High risk	Action: --Default--
Medium risk	Action: --Default--
Low risk	Action: --Default--
No Result	Action: --None--

Using the AntiVirus profile in a policy

1. Go to **Policy > IP Policy > IP Policy** and click **New**.
2. Under **Profiles**, select your newly created AntiVirus profile from the **AntiVirus** drop-down menu.
3. Click **Create**.



IP Based Policy

Enable: ●

Source: IP/netmask 0.0.0.0 / 0

Destination: IP/netmask 0.0.0.0 / 0

Action: Scan

Comment:

Profiles

Session: --None--

AntiSpam: --None--

AntiVirus: fortiguard-antivirus

Content: --None--

DLP: --None--

IP pool: --None--

Authentication and Access

Authentication type: --None--

Miscellaneous

○ Reject different SMTP sender identity for authenticated user

○ Sender identity verification with LDAP server for authenticated user

LDAP profile: --None--

○ Take precedence over recipient based policy match

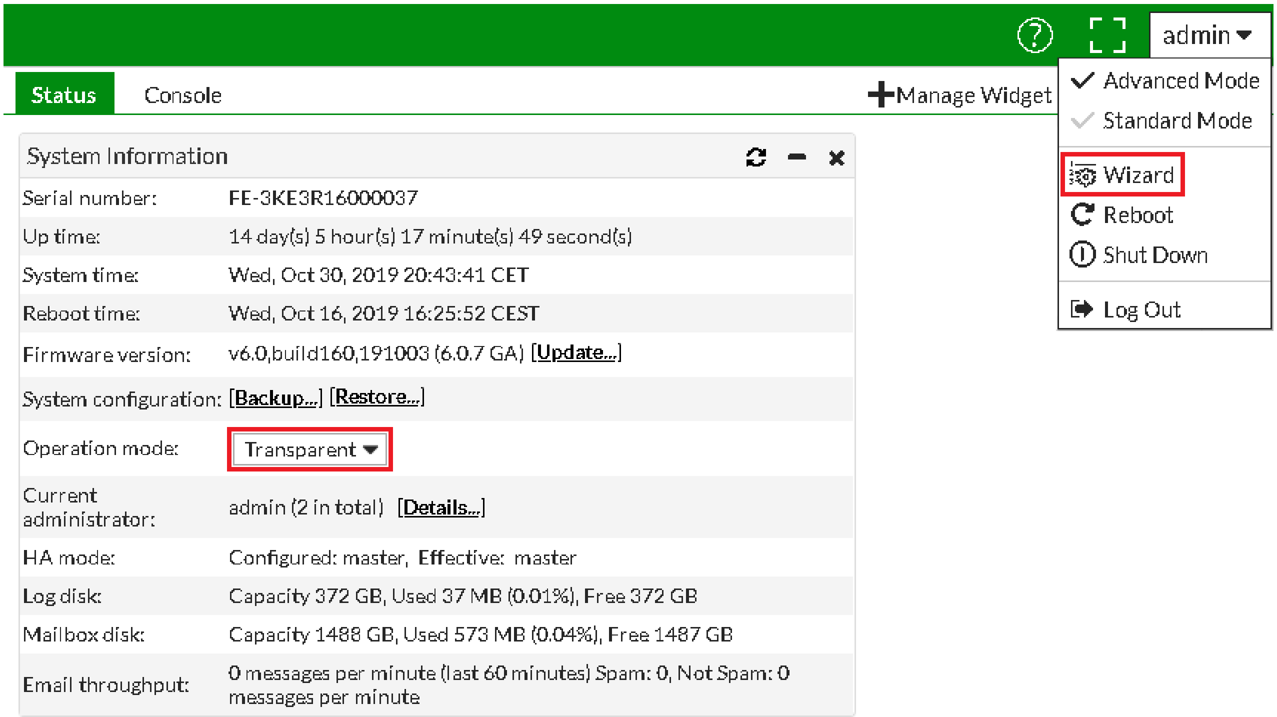
Preventing an ISP from being blocklisted

As a service provider you want to ensure that your IP address will not be blocklisted. Unfortunately, sometimes subscribers will send out spam, either on purpose, or accidentally, which will result in your IP being blocklisted. Thankfully, your FortiMail unit can help you avoid being blocklisted.

This recipe covers how to minimize the risk of innocent blocklisting.

Enabling transparent mode

1. Go to **Dashboard > Status**.
2. In the **System Information** widget, select **Transparent** from the **Operation mode** drop-down menu.
   A prompt appears stating that most settings will be reset to factory default after switching operation modes.
3. Click **OK** to confirm.
4. Click the FortiMail UI admin options and click **Wizard** to run the Quick Start Wizard.
5. Click **OK** to confirm.



Serial number:	FE-3KE3R16000037
Up time:	14 day(s) 5 hour(s) 17 minute(s) 49 second(s)
System time:	Wed, Oct 30, 2019 20:43:41 CET
Reboot time:	Wed, Oct 16, 2019 16:25:52 CEST
Firmware version:	v6.0,build160,191003 (6.0.7 GA) [Update...]
System configuration:	[Backup...] [Restore...]
Operation mode:	Transparent
Current administrator:	admin (2 in total) [Details...]
HA mode:	Configured: master, Effective: master
Log disk:	Capacity 372 GB, Used 37 MB (0.01%), Free 372 GB
Mailbox disk:	Capacity 1488 GB, Used 573 MB (0.04%), Free 1487 GB
Email throughput:	0 messages per minute (last 60 minutes) Spam: 0, Not Spam: 0 messages per minute

Configuring the connection with the RADIUS server

FortiMail uses RADIUS accounting records to combat spam and viruses originating from your network, reducing the likelihood that your public IP addresses will be blocklisted.

1. Configure the FortiMail unit as an auxiliary RADIUS server on your RADIUS server.
2. Ensure it sends the **Calling-Station-ID** and **Framed-IP-Address** attributes to the FortiMail unit.
3. Determine whether your RADIUS server sends the **Framed-IP-Address** attribute value in network order (for example, 192.168.1.10) or host order (for example, 10.1.168.192).
4. Verify that routing and firewall policies permit RADIUS accounting records to reach the FortiMail unit.

Testing the FortiMail

Once you are connected with the RADIUS server, you'll need to make sure the FortiMail unit is receiving the RADIUS records.

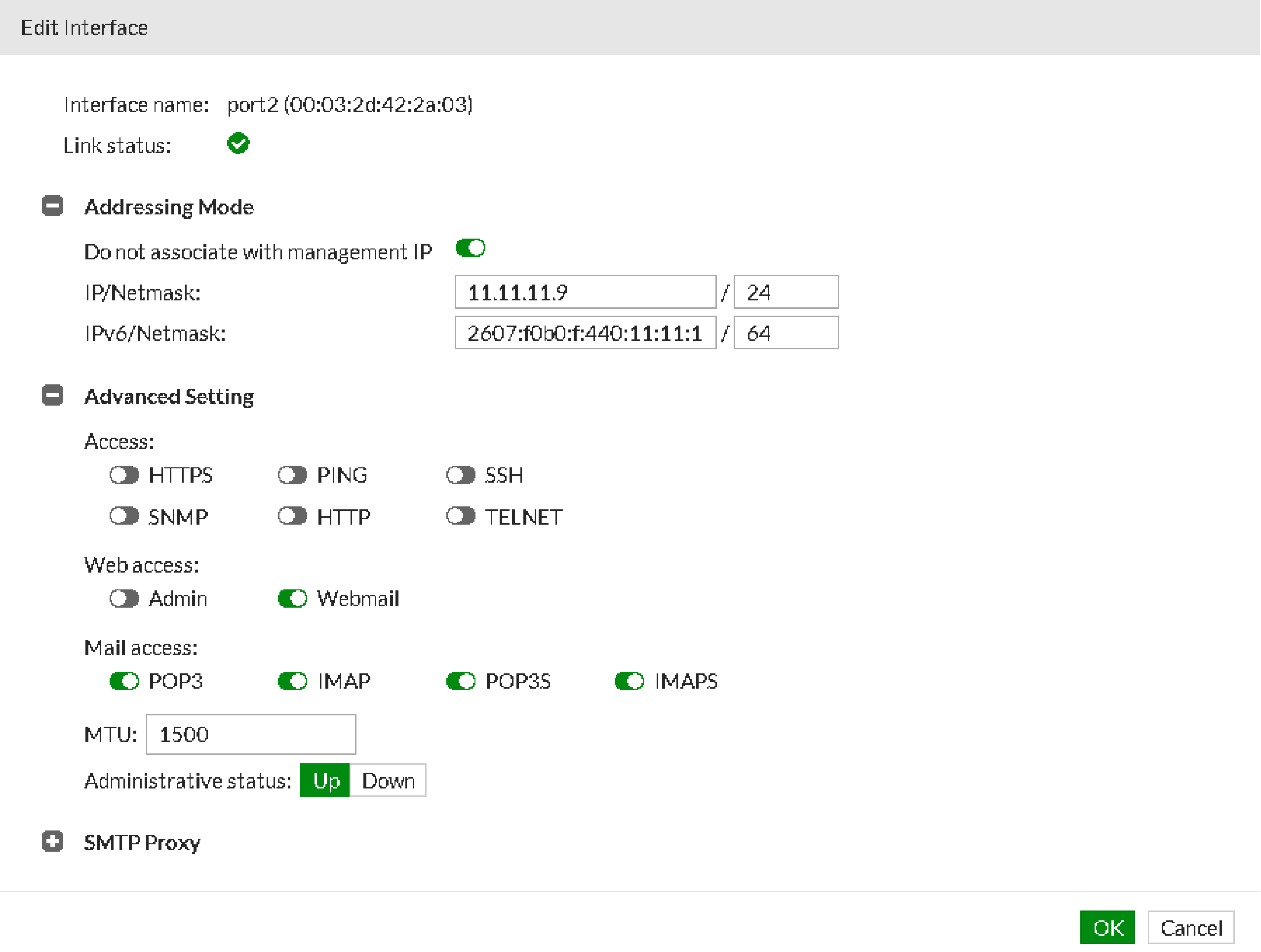
1. Go to **Dashboard > Console** and click to connect to the **CLI Console**.
2. Enter the following command to enable the FortiMail unit to receive RADIUS records by starting the endpoint reputation daemon:
```
config antispam settings
   set carrier-endpoint-attribute-status enable
end
```
3. Enter the following command to configure the RADIUS secret:
```
config antispam settings
   set carrier-endpoint-acc-secret enable
end
```
4. Enter the following command to configure whether to enable or disable the FortiMail unit to validate RADIUS requests using the RADIUS secret:
```
config antispam settings
   set carrier-endpoint-acc-validate enable
end
```
5. Enter the following command to configure whether or not the FortiMail unit will acknowledge accounting records:
```
config antispam settings
   set carrier-endpoint-acc-response {enable | disable}
end
```
6. Enter the following command to indicate that the RADIUS server will send the value of the **Framed-IP-Address** attribute in network order:
```
config antispam settings
   set carrier-endpoint-framed-ip-order {host-order | network-order}
end
```

Removing the network interfaces from the bridge

To remove port2 and port3 from the bridge repeat the following steps for each port.

1. Go to **System > Network > Interface** in the **Advanced Mode** of the FortiMail UI.
2. Select the port and click **Edit**.
3. Enable **Do not associate with management IP**. The interface is removed from the bridge, and may be configured with its own IP address.
4. Set **IP/Netmask** to the IP address and netmask of the network interface.
5. Under **Advanced Setting**, disable all administrative access protocols under **Access** and **Web access**, as shown in the example.

6. Click **Up**, and click **OK**.



Edit Interface

Interface name: port2 (00:03:2d:42:2a:03)

Link status: ✓

Addressing Mode

Do not associate with management IP ●

IP/Netmask: 11.11.11.9 / 24

IPv6/Netmask: 2607:f0b0:f:440:11:11:1 / 64

Advanced Setting

Access:

○ HTTPS ○ PING ○ SSH

○ SNMP ○ HTTP ○ TELNET

Web access:

○ Admin ● Webmail

Mail access:

● POP3 ● IMAP ● POP3S ● IMAPS

MTU: 1500

Administrative status: [✓ Up] Down

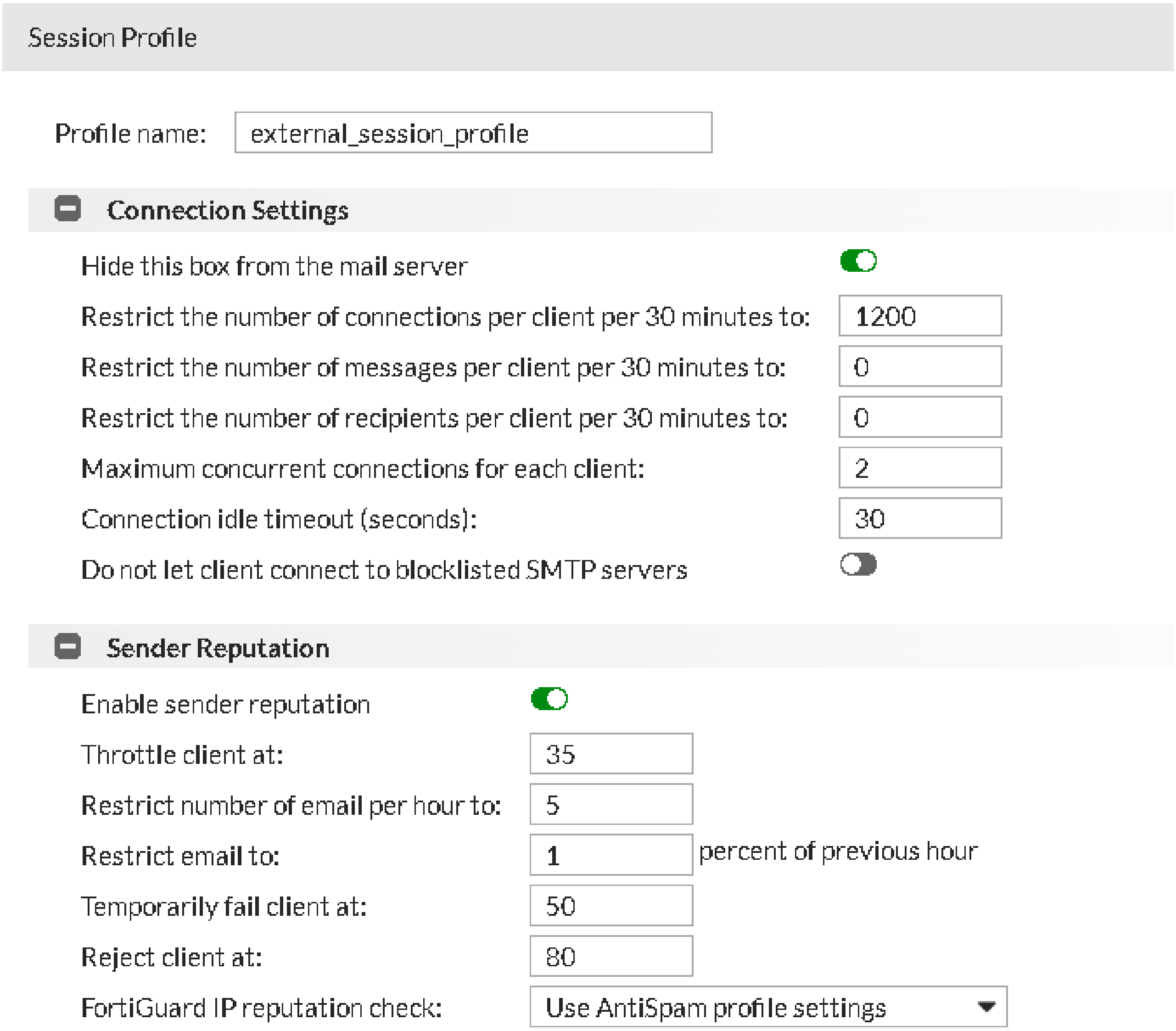
SMTP Proxy

Configuring the session profiles

Follow the steps below to create two session profiles for connections: one profile for external (example shown below), and another profile for internal SMTP clients.

For more detailed information about session profile configuration settings, see the FortiMail Administration Guide.

1. Go to **Profile > Session > Session** and click **New**.
2. Enter a **Profile name**.
3. Under **Connection Settings**, enable **Hide this box from the mail server** to preserve the IP address or domain name of the SMTP client.
4. Under **Sender Reputation**, click **Enable sender reputation** and leave the settings to their default values.



Session Profile

Profile name: external_session_profile

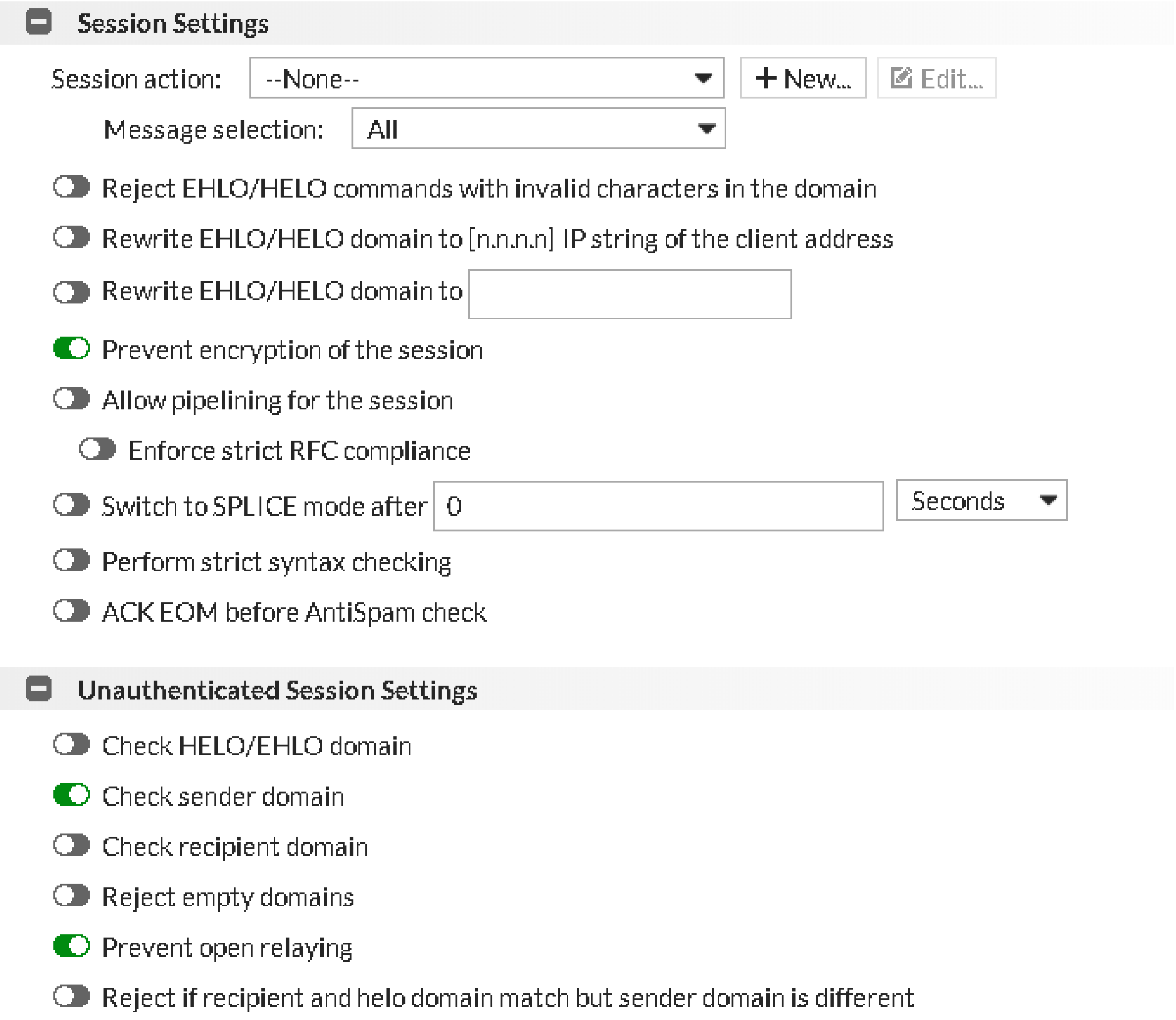
⊟ Connection Settings

Hide this box from the mail server	●
Restrict the number of connections per client per 30 minutes to:	1200
Restrict the number of messages per client per 30 minutes to:	0
Restrict the number of recipients per client per 30 minutes to:	0
Maximum concurrent connections for each client:	2
Connection idle timeout (seconds):	30
Do not let client connect to blocklisted SMTP servers	○

⊟ Sender Reputation

Enable sender reputation	●
Throttle client at:	35
Restrict number of email per hour to:	5
Restrict email to:	1 percent of previous hour
Temporarily fail client at:	50
Reject client at:	80
FortiGuard IP reputation check:	Use AntiSpam profile settings ▾

5. Under **Session Settings**, enable **Prevent encryption of the session** so that STARTTLS/MD5 commands are blocked and email connections cannot be TLS-encrypted.
6. Under Unauthenticated Session Settings, enable Prevent open relaying.
7. Click **Create**.



Session Settings

Session action: --None--

Message selection: All

○ Reject EHLO/HELO commands with invalid characters in the domain

○ Rewrite EHLO/HELO domain to [n.n.n.n] IP string of the client address

○ Rewrite EHLO/HELO domain to

● Prevent encryption of the session

○ Allow pipelining for the session

○ Enforce strict RFC compliance

○ Switch to SPLICE mode after 0 Seconds

○ Perform strict syntax checking

○ ACK EOM before AntiSpam check

Unauthenticated Session Settings

○ Check HELO/EHLO domain

● Check sender domain

○ Check recipient domain

○ Reject empty domains

● Prevent open relaying

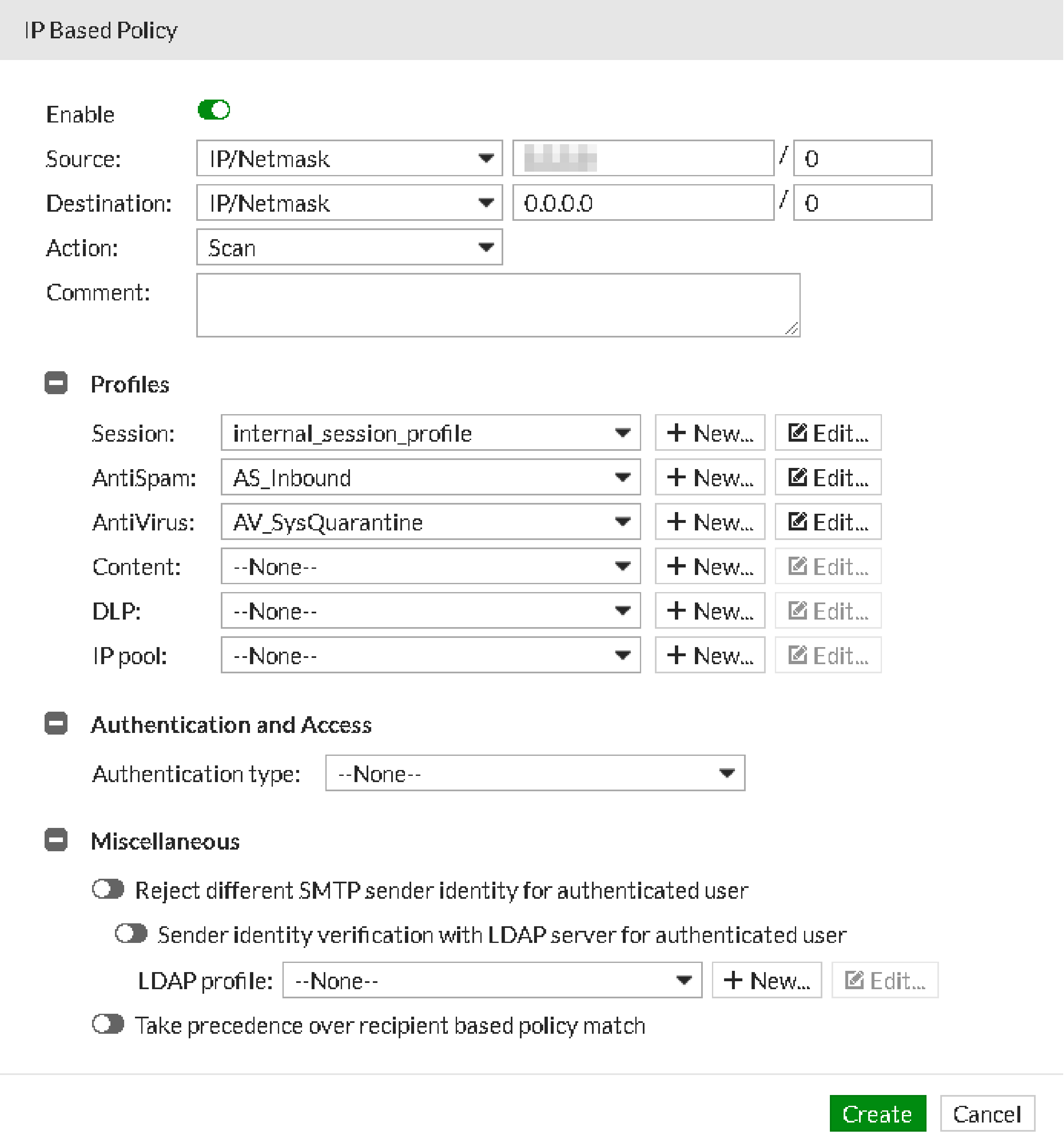
○ Reject if recipient and helo domain match but sender domain is different

Configuring IP-based policies

First, configure the IP-based policy for connections from internal SMTP clients.

1. Go to **Policy > IP Policy > IP Policy** and click **New**.
2. Click **Enable**.
3. Set **Source** to the IP address and netmask of your subscriber network.
4. Under **Profile**, select the **internal_session_profile** from the **Session** drop-down list.

5. Click **Create**.



IP Based Policy

Enable: ●

Source: IP/Netmask [redacted] / 0

Destination: IP/Netmask 0.0.0.0 / 0

Action: Scan

Comment:

Profiles

Session:	internal_session_profile	+ New...	Edit...
AntiSpam:	AS_Inbound	+ New...	Edit...
AntiVirus:	AV_SysQuarantine	+ New...	Edit...
Content:	--None--	+ New...	Edit...
DLP:	--None--	+ New...	Edit...
IP pool:	--None--	+ New...	Edit...

Authentication and Access

Authentication type: --None--

Miscellaneous

○ Reject different SMTP sender identity for authenticated user

○ Sender identity verification with LDAP server for authenticated user

LDAP profile: --None-- + New... Edit...

○ Take precedence over recipient based policy match

Configure the IP-based policy for connections from external SMTP clients.

1. Go to **Policy > IP Policy > IP Policy**. Select the default policy whose **Source** and **Destination** are both 0.0.0.0/0 and click **Edit**.
2. Under **Profiles**, select the **external_session_profile** from the **Session** drop-down menu.
3. Click **OK**.

Configuring the outgoing proxy

When operating in transparent mode, the FortiMail unit can use either transparent proxies or an implicit relay to inspect SMTP connections. If connection pick-up is enabled for connections on that network interface, the FortiMail unit can scan and process the connection. If not enabled, the FortiMail unit can either block or permit the connection to pass through unmodified.

First, configure the outgoing proxy pick-up settings.

1. Go to **System > Mail Setting > Proxies**.
2. Enable **Use client-specified SMTP server to send email** and click **Apply**.
3. Go to **System > Network > Interface**.
4. Edit SMTP proxy settings for both port2 and port3. Under **SMTP Proxy**:
   - Set **Incoming connections** to **Drop**.
   - Set **Outgoing connections** to **Proxy**.
   - Disable **Local connections**.

Configuring policy-based routes on the router

After you have configured the FortiMail settings, you must create policy routes on the router to redirect the SMTP traffic (from and to the subscribers) to the FortiMail unit for scanning.

For example, on a FortiGate unit as the router/firewall, go to **Router > Policy Route** to create two routes: one for the external-to-subscribers SMTP traffic and one for the subscribers-to-external SMTP traffic.

For more information, see the FortiGate Handbook.

Protecting against email impersonation in FortiMail

Email impersonation, or Business Email Compromise (BEC), is one of the main problems facing the safety of many businesses today. Impersonators create email headers to deceive the recipient into believing the sender is from a legitimate and trusted source.

If you have a Fortinet Enterprise Advanced Threat Protection (ATP) bundle license, FortiMail provides you a solution to fight against email impersonation by mapping high valued target display names with correct email addresses.

For example, if an external spammer wants to impersonate the CEO of your company (CEO@company.com), the spammer places “CEO ABC <ceo@external.com>” in the email header and sends the message to the user. If FortiMail is configured with a manual entry “CEO ABC” to “ceo@company.com” mapping in the impersonation profile to indicate the correct display name and email pair, or it has learned the pair through the dynamic process, then that email is detected by impersonation analysis.

This recipe guides you through the easy to follow process of creating and implementing an impersonation profile to better protect your network.

There are two types of mapping:

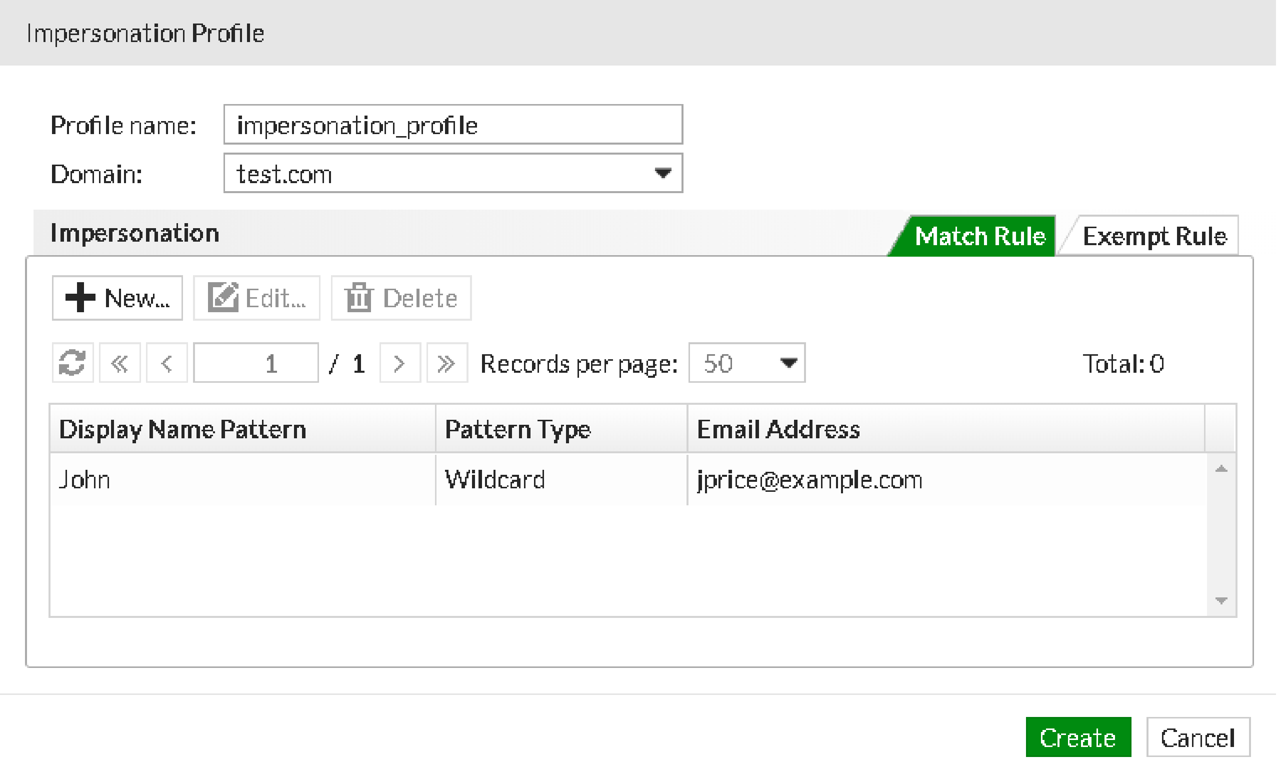
- **Manual**: You manually enter mapping entries and create impersonation analysis profiles as described below and then enable the impersonation profile in an antispam profile. Eventually you apply the antispam profile in the IP-based or recipient-based policies.
- **Dynamic**: FortiMail Mail Statistics Service can automatically learn the mapping.

Creating an impersonation analysis profile

Create an impersonation profile and add display names and email addresses to map.

1. Go to **Profile > AntiSpam > Impersonation** and click **New**.
2. Enter an appropriate **Profile name**.
3. Select a **Domain** from the drop-down list.
4. Under **Impersonation**, click **New** to add individuals within your business you know to be safe.
5. Enter a **Display name pattern**, set **Pattern type** to either **Wildcard** or **Regular expression**, and enter an **Email address** to be mapped to the display name. Click **Create**.

6. Click **Create** again to complete the impersonation profile.



Impersonation Profile

Profile name:	impersonation_profile
Domain:	test.com

Impersonation

Display Name Pattern	Pattern Type	Email Address
John	Wildcard	jprice@example.com

Activating the impersonation profile

1. Go to **Profile > AntiSpam > AntiSpam** and click **New**, or edit an existing profile.
2. Under **Scan Configurations**, enable **Impersonation analysis**.
3. Set an appropriate **Action**, and click **Create** or **OK**.
4. When you create an IP policy or recipient policy, make sure to select the antispam profile that contains the impersonation analysis profile.

Viewing the impersonation analysis logs

When messages are sent using a forged display name, the **Header From** is compared to the entry in the impersonation analysis profile. If the display name does not match the email address, the FortiMail unit identifies the impersonation attempt and quarantines the message.

1. Go to **Monitor > Log > History**.
2. Select the desired entry for inspection and click **View**.

Configuring dynamic scanning

In addition to manually entering mapping entries and creating impersonation analysis profiles, FortiMail Mail Statistics Service can automatically learn the mapping in the incoming email **Header To** fields and track the mapping dynamically.

To use the FortiMail manual, dynamic, or both impersonation analysis scanning, enter the following command:

```
config antispam settings
   set impersonation-analysis dynamic manual
end
```

By default, FortiMail uses manual analysis only.

Also enable the FortiMail Mail Statistics Service with the following command. This service is disabled by default:

```
config system global
   set mailstat-service enable
end
```

Preparing DMARC checking for outbound email

This recipe describes the outbound email Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), and Domain-based Message Authentication, Reporting & Conformance (DMARC) preparation on FortiMail and the DNS server for verification by the receiving email servers.

Email signing requires up-to-date SPF, DKIM, and DMARC TXT records within the DNS server:

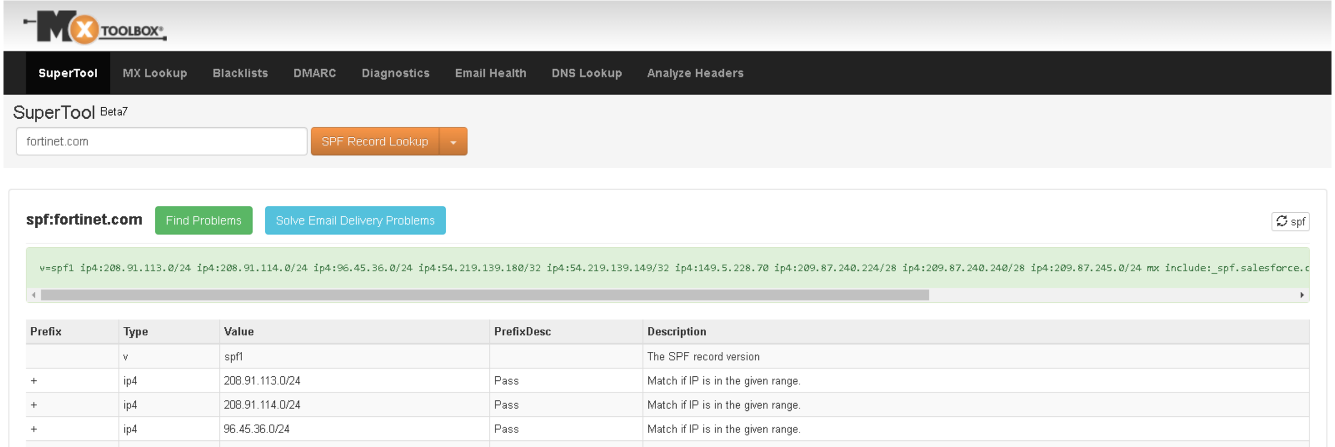
- For outbound email, SPF records indicate who is authorized to send email on your behalf. SPF records contain the client IP addresses of the domains' authorized senders. These domains are checked until an authorized IP address match occurs. If the test fails, the email is identified as spam. DNS records must be kept up-to-date.
- DKIM records digitally sign outbound emails to prove that the email has not been tampered with in transit. This is achieved through both a public key and a private key. The public key is what is published to the DNS record, so receiving MTAs can download the key and validate the signature.
- On the receiver's end, DMARC records provide a form of feedback as to whether SPF and DKIM passed. For Fortinet as an example, DMARC passes if either SPF or DKIM pass. Otherwise, if both SPF and DKIM fail, DMARC takes an action of either none, quarantine, or reject.

Note that SPF performs its check using the Mail From address, or the RFC5321.MailFrom (envelope) address. DMARC enhances SPF by performing its check against the From address, or the RFC5322.From (header) address.

This prevents situations where messages can pass an SPF check, but spoof its RFC5322.From sender address.

For more information, see identifier alignment information at RFC 7489.

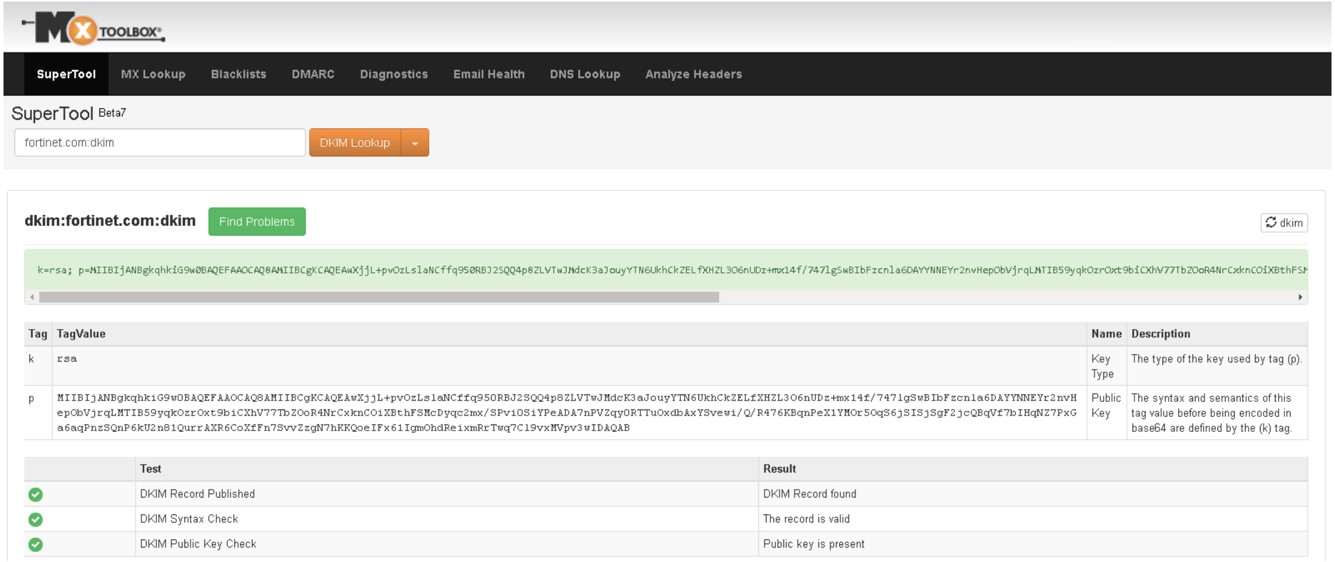
Below are examples, taken from publicly accessible DNS records at mxtoolbox.com, of the three TXT records required for a given domain (in this example, fortinet.com):



spf:fortinet.com

```
v=spf1 ip4:208.91.113.0/24 ip4:208.91.114.0/24 ip4:96.45.36.0/24 ip4:54.219.139.180/32 ip4:54.219.139.149/32 ip4:149.5.228.70 ip4:209.87.240.224/28 ip4:209.87.240.240/28 ip4:209.87.245.0/24 mx include:_spf.salesforce.c
```

Prefix	Type	Value	PrefixDesc	Description
	v	spf1		The SPF record version
+	ip4	208.91.113.0/24	Pass	Match if IP is in the given range.
+	ip4	208.91.114.0/24	Pass	Match if IP is in the given range.
+	ip4	96.45.36.0/24	Pass	Match if IP is in the given range.

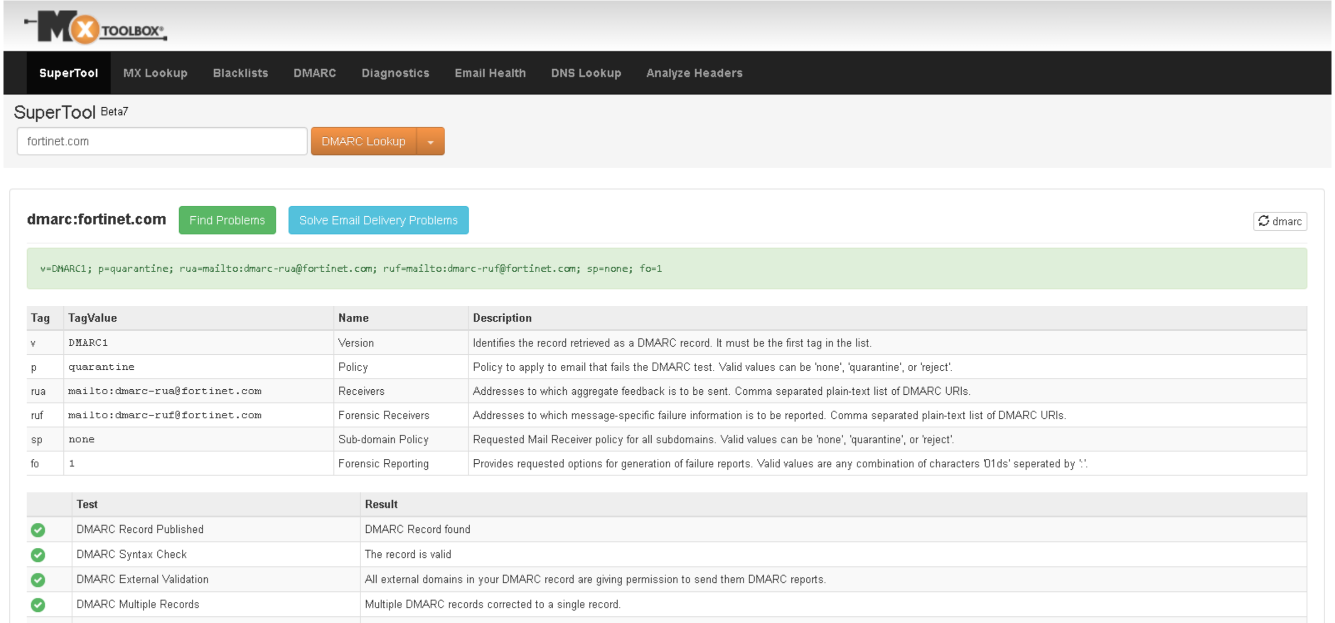


dkim:fortinet.com:dkim

```
k=rsa; p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAwXjjL+pvOzLslaNCffq950RBJ2SQQ4p8ZLVTwJMdcK3aJouyYTN6UkhCkZELfXHZL3O6nUDz+mx14f/747lgSwBIbFzcnla6DAYYNNEYr2nvHepObVjrqLMTIB59yqkOzrOxt9biCXhV77TbZOoR4NrCxknCOiXBthFSM
```

Tag	TagValue	Name	Description
k	rsa	Key Type	The type of the key used by tag (p).
p	MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAwXjjL+pvOzLslaNCffq950RBJ2SQQ4p8ZLVTwJMdcK3aJouyYTN6UkhCkZELfXHZL3O6nUDz+mx14f/747lgSwBIbFzcnla6DAYYNNEYr2nvHepObVjrqLMTIB59yqkOzrOxt9biCXhV77TbZOoR4NrCxknCOiXBthFSMcDyqc2mx/SPvi0SiYPeADA7nPVZqyORTTuOxdbAxYSvewi/Q/R476KBqnPeX1YMOr5OqS6jSISjSgF2jcQBqVf7bIHqNZ7PxGa6aqPnzSQnP6kU2n81QurrAXR6CoXfFn7SvvZzgN7hKKQoeIFx61IgmOhdReixmRrTwq7C19vxMVpv3wIDAQAB	Public Key	The syntax and semantics of this tag value before being encoded in base64 are defined by the (k) tag.

	Test	Result
✓	DKIM Record Published	DKIM Record found
✓	DKIM Syntax Check	The record is valid
✓	DKIM Public Key Check	Public key is present



dmarc:fortinet.com

```
v=DMARC1; p=quarantine; rua=mailto:dmarc-rua@fortinet.com; ruf=mailto:dmarc-ruf@fortinet.com; sp=none; fo=1
```

Tag	TagValue	Name	Description
v	DMARC1	Version	Identifies the record retrieved as a DMARC record. It must be the first tag in the list.
p	quarantine	Policy	Policy to apply to email that fails the DMARC test. Valid values can be 'none', 'quarantine', or 'reject'.
rua	mailto:dmarc-rua@fortinet.com	Receivers	Addresses to which aggregate feedback is to be sent. Comma separated plain-text list of DMARC URIs.
ruf	mailto:dmarc-ruf@fortinet.com	Forensic Receivers	Addresses to which message-specific failure information is to be reported. Comma separated plain-text list of DMARC URIs.
sp	none	Sub-domain Policy	Requested Mail Receiver policy for all subdomains. Valid values can be 'none', 'quarantine', or 'reject'.
fo	1	Forensic Reporting	Provides requested options for generation of failure reports. Valid values are any combination of characters '01ds' seperated by ':'.

	Test	Result
✓	DMARC Record Published	DMARC Record found
✓	DMARC Syntax Check	The record is valid
✓	DMARC External Validation	All external domains in your DMARC record are giving permission to send them DMARC reports.
✓	DMARC Multiple Records	Multiple DMARC records corrected to a single record.

In this example, the appropriate text records for SPF, DKIM, and DMARC are retrieved for the domain fortinet.com. These records are used to update the DNS server, and an email is sent from a Fortinet account to a Gmail account (from fortinet.com to gmail.com) to prove the email passed successfully.

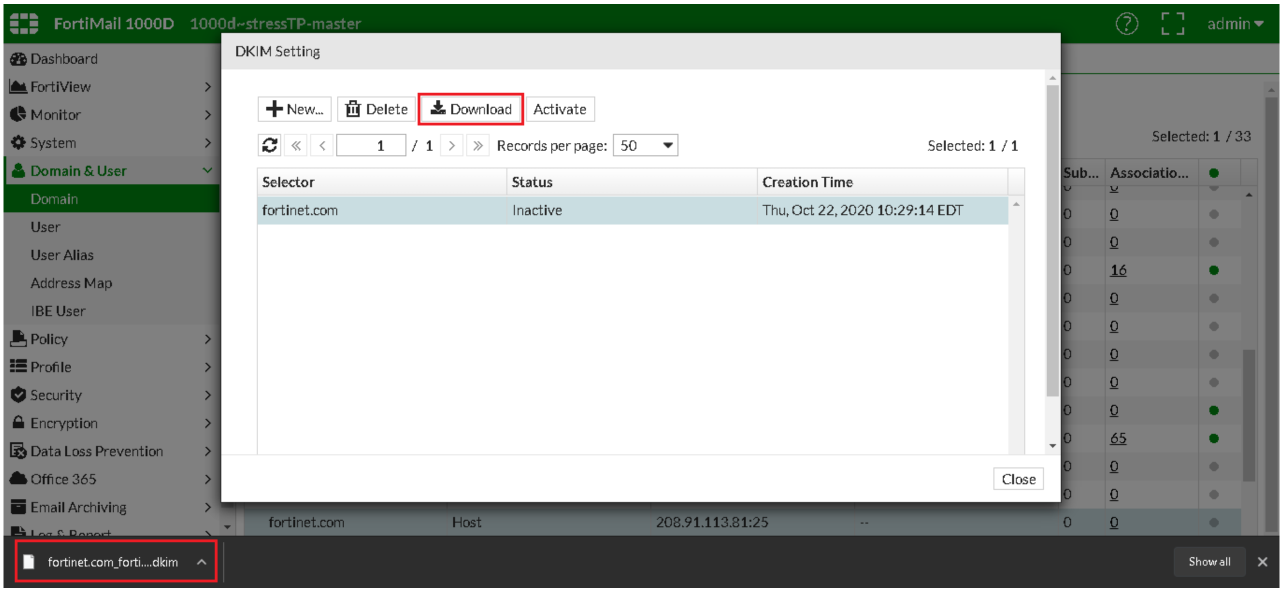
For more information about these email authentication protocols, see the FortiMail Administration Guide. For a recipe regarding email checking, see Configuring incoming email DMARC checking with SPF and DKIM.

Enabling DKIM signing on FortiMail

In order to sign outgoing mail with DKIM signatures, you must configure the protected domain. In this example, a selector and DKIM key is generated for fortinet.com.

Note that DKIM signing settings only appear when configuring an existing protected domain.

1. Go to **Domain & User > Domain > Domain** and edit an existing profile.
2. Under **Advanced Setting**, click **DKIM Setting**.
3. Click **New**.
4. Enter a name in the **New selector** field.
   Note that the selector name must match its corresponding domain name (in this example, fortinet.com)
5. Set **DKIM key** to **Auto Generation**. The key pair will be automatically generated and the public key exported for publication on a DNS server.
6. Click **OK**.
7. The new selector appears. Select the newly created selector and click **Download** to download the domain key DKIM file.



Selector	Status	Creation Time
fortinet.com	Inactive	Thu, Oct 22, 2020 10:29:14 EDT

8. From the **DKIM Setting** window in FortiMail, select the newly created selector and click **Activate**.
9. Click **Close**, and click **OK**.

In the next step, along with the SPF and DMARC record, the public DKIM key is published by inserting the exported DNS record into the DNS zone file of the DNS server that resolves this domain name.

Retrieving public DNS record information

Below are the public DNS records for Fortinet. These, among others, can be accessed from mxtoolbox.com. Use the appropriate records you need in order to receive emails only from those you trust as authorized senders.

SPF record:

The following SPF record contains the client IP addresses who are authorized senders of permitted domains. The included domains listed are continuously checked until an authorized IP address match occurs, as highlighted by the red-text. The `-all` signifies that any other email that comes from outside those authorized senders listed comes from an unauthorized sender.

```
dig -t txt fortinet.com @8.8.8.8
; <<>> DiG 9.9.5-3ubuntu0.19-Ubuntu <<>> -t txt fortinet.com @8.8.8.8
;; global options: +cmd
;; Got answer:
```

```
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 54525
;; flags: qr rd ra; QUERY: 1, ANSWER: 7, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;fortinet.com. IN TXT
;; ANSWER SECTION:
fortinet.com. 21599 IN TXT "v=spf1 ip4:208.91.113.0/24 ip4:208.91.114.0/24 ip4:96.45.36.0/24
      ip4:54.219.139.180/32 ip4:54.219.139.149/32 ip4:149.5.228.70 ip4:209.87.240.224/28
      ip4:209.87.240.240/28 ip4:209.87.245.0/24 mx include:" "_spf.salesforce.com
      include:fortinet.co.jp include:obmail.socious.net include:freshdesk.fortinet.com -all"
fortinet.com. 21599 IN TXT "6c5446a498ce4d53b989cfd26942be56"
fortinet.com. 21599 IN TXT
      "GU471ZEfO/K1S60mBByKjl+gpL0jPAE+zYYlpa0mlLLm6b01NReZ+BXBoX2f1dQ8xUkcMcEYz6ficlvvOZwTug=
      ="
fortinet.com. 21599 IN TXT "MS=3EDB3515616567F5F3B65CD58B2C045CD4F1D82F"
fortinet.com. 21599 IN TXT
      "pardot872291=187e99aeea474c37f2966e1aac54b813b2d9331ae23e3d2a17fe61672746f72a"
fortinet.com. 21599 IN TXT "facebook-domain-verification=aakjubmhk3oxdlv2efp7faayfcz8bf"
fortinet.com. 21599 IN TXT "MS=MS65931290"
;; Query time: 153 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Wed Oct 07 09:39:09 EDT 2020
;; MSG SIZE rcvd: 751
```

DKIM record:

The following DKIM record contains the published public key, as highlighted by the red-text. This was generated in FortiMail earlier, and is used to sign and decrypt emails.

```
$ dig -t TXT dkim._domainkey.fortinet.com @8.8.8.8
; <<>> DiG 9.9.5-3ubuntu0.19-Ubuntu <<>> -t TXT dkim._domainkey.fortinet.com @8.8.8.8
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 52891
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;dkim._domainkey.fortinet.com. IN TXT
;; ANSWER SECTION:
dkim._domainkey.fortinet.com. 21599 IN TXT "t=y\; k=rsa\; p="
      "MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAwXjjL+pvOzLslaNCffq950RBJ2SQQ4p8ZLVTwJMdcK3a
      JouyYTN6UkhCkZELfXHZL3O6nUDz+mx14f/747lgSwBIbFzcnla6DAYYNNEYr2nvHepObVjrqLMTIB59yqkOzrOxt
      9biCXhV77TbZOoR4NrCxknC"
      "OiXBthFSMcDyqc2mx/SPvi0SiYPeADA7nPVZqy0RTTuOxdbAxYSvewi/Q/R476KBqnPeX1YMOr5OqS6jSISjSgF2
      jcQBqVf7bIHqNZ7PxGa6aqPnzSQnP6kU2n81QurrAXR6CoXfFn7SvvZzgN7hKKQoeIFx61IgmOhdReixmRrTwq7Cl
      9vxMVpv3wIDAQAB"
;; Query time: 110 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Wed Oct 07 09:47:13 EDT 2020
;; MSG SIZE rcvd: 478
```

DMARC record:

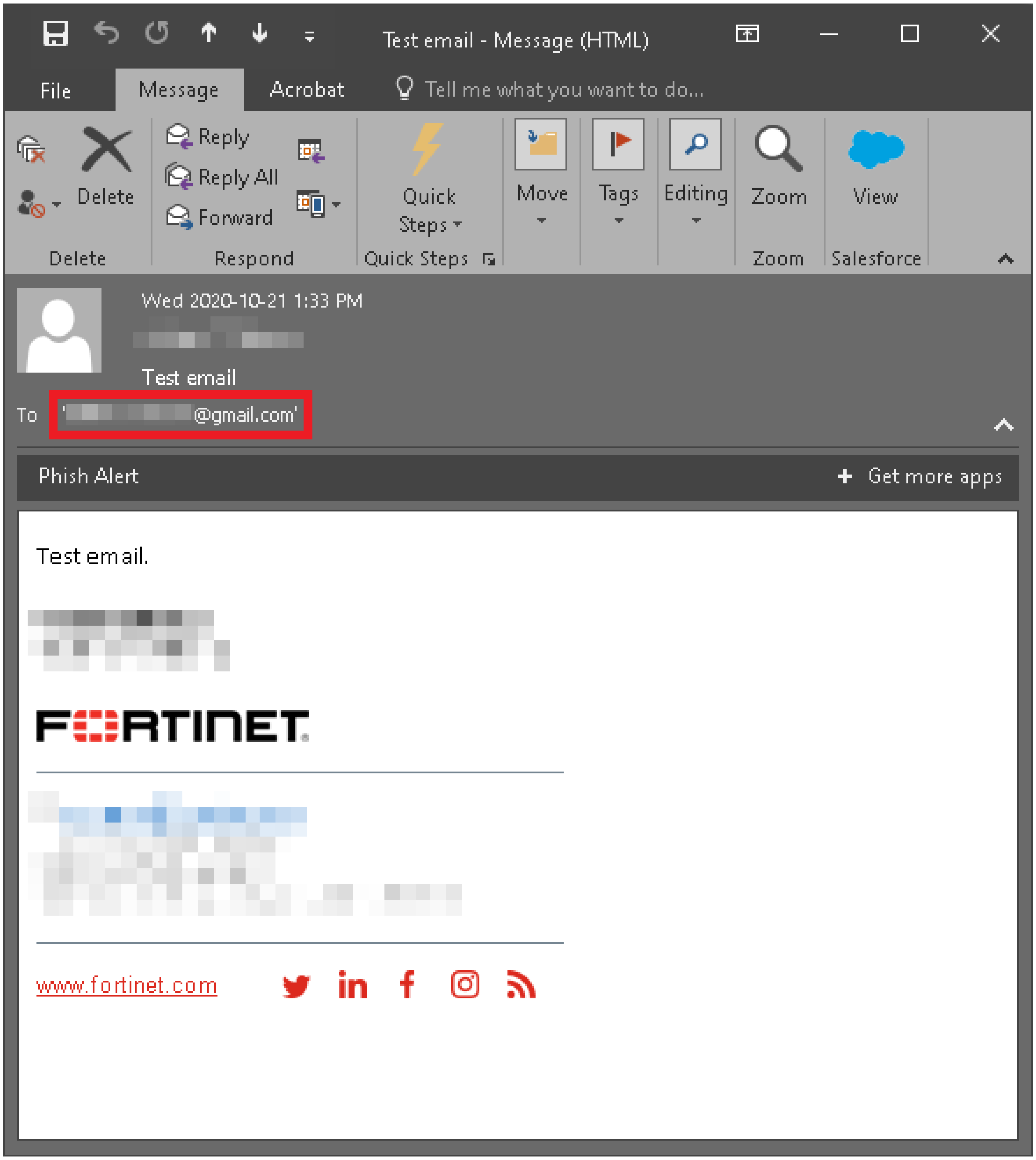
The following DMARC record contains the default action to take if both SPF and DKIM fail (in this case, `p=quarantine`), as highlighted by the red-text. The RUA and RUF records are used to send XML files to record SPF and DKIM feedback.

```
dig -t txt _dmarc.fortinet.com @8.8.8.8
; <<>> DiG 9.9.5-3ubuntu0.19-Ubuntu <<>> -t txt _dmarc.fortinet.com @8.8.8.8
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 144
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;_dmarc.fortinet.com. IN TXT
;; ANSWER SECTION:
_dmarc.fortinet.com. 599 IN TXT "v=DMARC1\; p=quarantine\; rua=mailto:dmarc-rua@fortinet.com\;
     ruf=mailto:dmarc-ruf@fortinet.com\; sp=none\; fo=1"
;; Query time: 100 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Wed Oct 07 09:40:31 EDT 2020
;; MSG SIZE rcvd: 168
```

Testing email signing and verification

For this example, an email can be sent from a Gmail account to a Fortinet account, and the email's Internet headers can show successful SPF and DKIM signing.

1. Send a test email from your domain to a Gmail address.



Wed 2020-10-21 1:33 PM

[redacted]

Test email

To '[redacted]@gmail.com'

Test email.

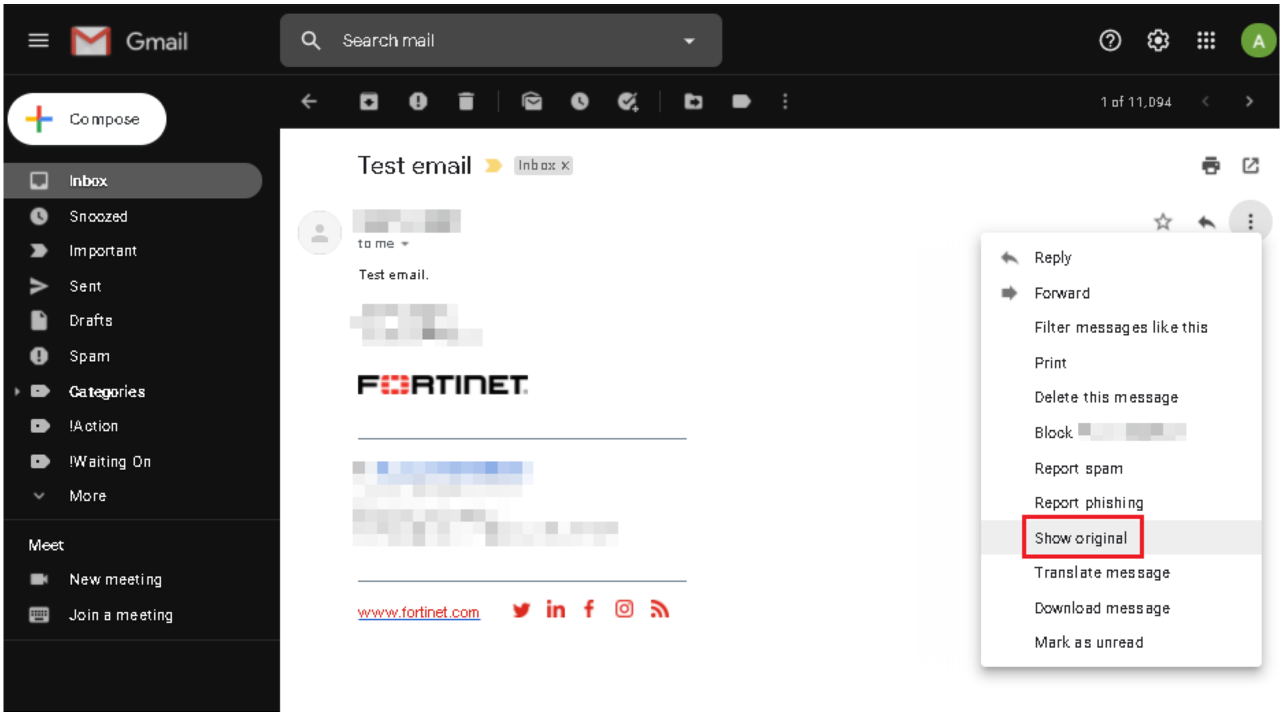
[redacted]

FORTINET

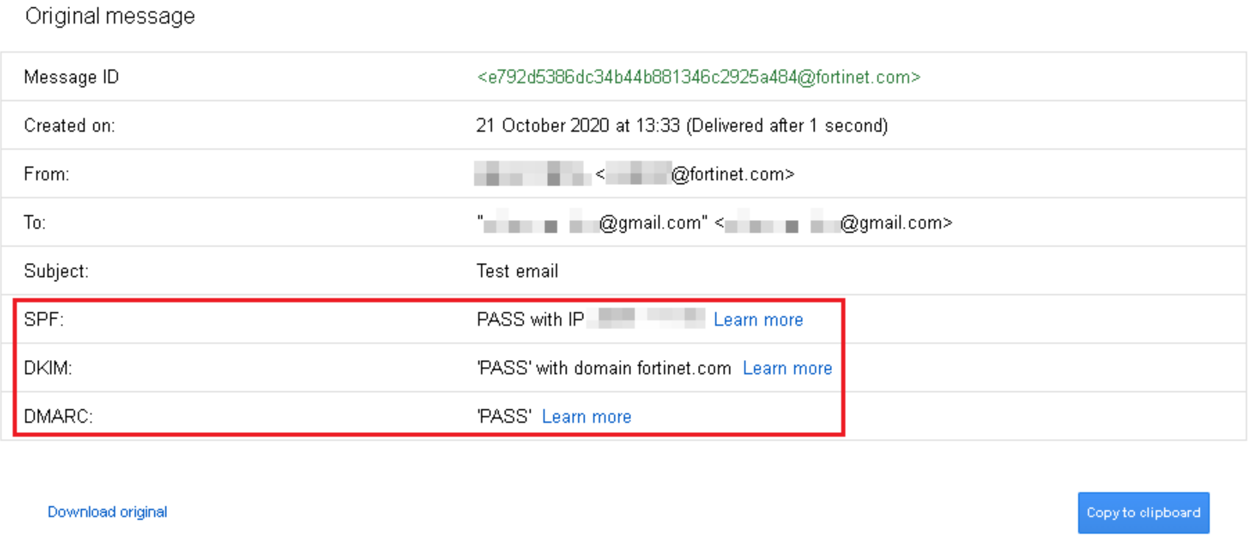
[redacted]

www.fortinet.com

2. Once the email has been received, open the email in Gmail and click **Show original**.



3. Among the various details, you can see that the email passed SPF, DKIM, and DMARC.



Original message

Message ID	<e792d5386dc34b44b881346c2925a484@fortinet.com>
Created on:	21 October 2020 at 13:33 (Delivered after 1 second)
From:	[redacted] <[redacted]@fortinet.com>
To:	"[redacted]@gmail.com" <[redacted]@gmail.com>
Subject:	Test email
SPF:	PASS with IP [redacted] Learn more
DKIM:	'PASS' with domain fortinet.com Learn more
DMARC:	'PASS' Learn more

Below this summary, you can view the email's full text-readout of properties, including email headers and other diagnostic information. Among this information is the `Authentication-Results`, showing the specific SPF, DKIM, and DMARC results:

```
Authentication-Results: mx.google.com;
   dkim=pass header.i=@fortinet.com header.s=dkim header.b=Lcxh1a5H;
   spf=pass (google.com: domain of example@fortinet.com designates <ip-address> as
         permitted sender) smtp.mailfrom=example@fortinet.com;
   dmarc=pass (p=QUARANTINE sp=NONE dis=NONE) header.from=fortinet.com
```

Best practices

This section contains information regarding best practices while configuring ForttiMail.

Resetting a lost administrator password

Periodically a situation arises where your FortiMail unit needs to be accessed or the administrator account's password needs to be changed but no one with the existing password is available. If physical access to the device is possible and with a few other tools, the password can be reset.

This procedure will require the reboot of the FortiMail unit.

FortiMail versions 6.0.8 and 6.2.3 introduce a new CLI command allowing you to enable or disable administrator password recovery:

```
config system global
   set admin-maintainer {enable | disable}
end
```

The following procedure requires `admin-maintainer` to be set to `enable`.

Administrators with physical access to a FortiMail unit can use a console cable and the maintainer administrator account to log into the CLI. The maintainer account allows you to log into a FortiMail unit if you have lost all administrator passwords.

Once logged into the FortiMail unit with the maintainer account, you can reset the passwords of super-admin profile accounts, or enter the `execute factoryreset` command to return the FortiMail unit to its default configuration. This can be useful if the admin administrator account was deleted.

The `admin-maintainer` command is enabled by default. The methodology for using the maintainer account is publicly available. As long as someone with physical access to the device has the serial number of the device, which is labeled on the device, the admin administrator account password can be changed and access to the FortiMail unit is granted.

If this is an unacceptable risk to your specific environment (especially where the hardware is not physically secured), you can disable the command. However, if the feature is disabled, and the password gets lost without having someone else that can log in as a super-admin, you will have no options to restore access.

Requirements:

- Console cable
- Terminal software such as Putty.exe (Windows) or Terminal (MacOS)
- Serial number of the FortiGate device

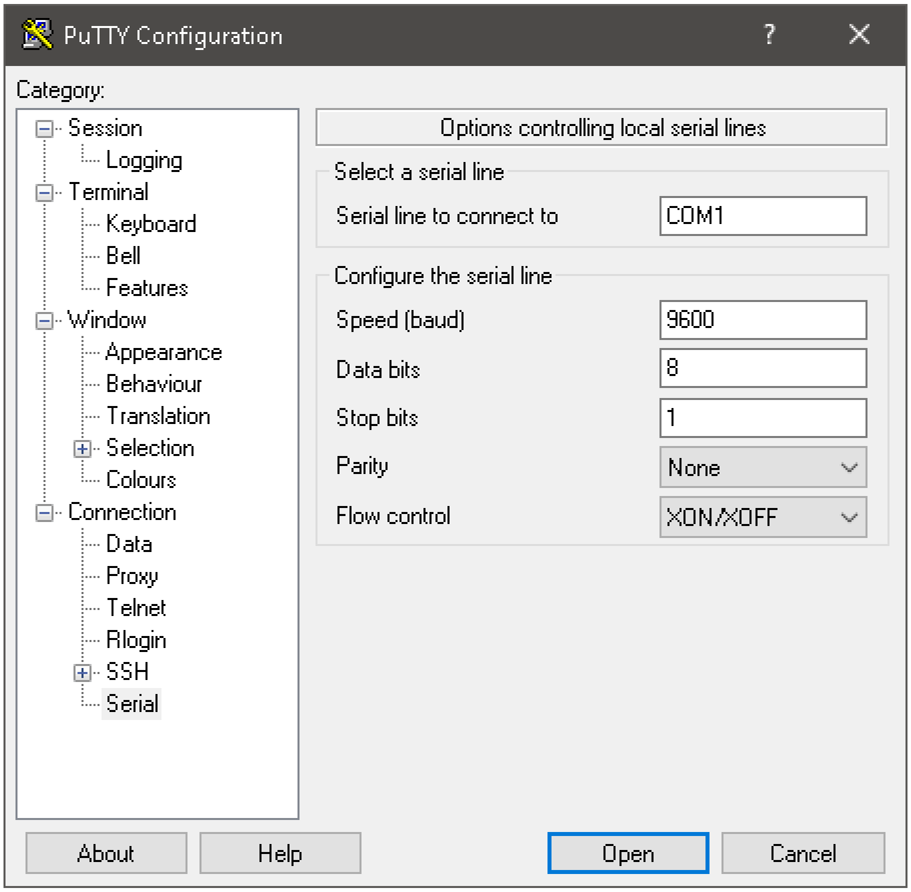
Physically connect the FortiMail unit

1. Connect the computer to the FortiMail via the Console port on the unit.
   In most units this is done either by a Serial cable or a RJ-45 to Serial cable.

2. For virtual instances of FortiMail (that do not have any physical port to connect) use the supplied VM Hosts' console connection utility.

Connect to the FortiMail unit using terminal software

1. Start the terminal software, for example PuTTY.
2. Open the serial connection settings and enter the following:
   - **COM port/serial line**: The appropriate COM port
   - **Speed (baud)**: 9600
   - **Data bits**: 8
   - **Stop bits**: 1
   - **Parity**: None
   - **Flow control**: No hardware flow control
3. Click **Open**.



Options controlling local serial lines

Select a serial line

Serial line to connect to: COM1

Configure the serial line

Speed (baud): 9600

Data bits: 8

Stop bits: 1

Parity: None

Flow control: XON/XOFF

4. The FortiMail unit should then respond with its name or hostname (if it does not try pressing "Enter").
5. Reboot the FortiMail unit. If there is no power button, disconnect the power adapter and reconnect it after 10 seconds.

Plugging in the power too soon after unplugging it can cause corruption in the memory in some units.

Log in using the maintainer account

1. Once the FortiMail unit has finished rebooting, on the login prompt, enter `maintainer`.
2. The password is `bcpb` plus the serial number of the unit. Make sure to enter the serial number in upper-case format. For example:
   ```
   bcpbFE900FT918******
   ```

After the device reboots, there is only 60 seconds or less to type in the username and password. It is recommended to have the credentials ready in a text editor to copy and paste them into the login screen when required. There is no indicator of when the time runs out so it might take more than one attempt to succeed.

Change the admin password

1. Once logged in as the maintainer, enter the following CLI command:
   ```
   config system admin
      edit admin
         set password <password_str>
   end
   ```

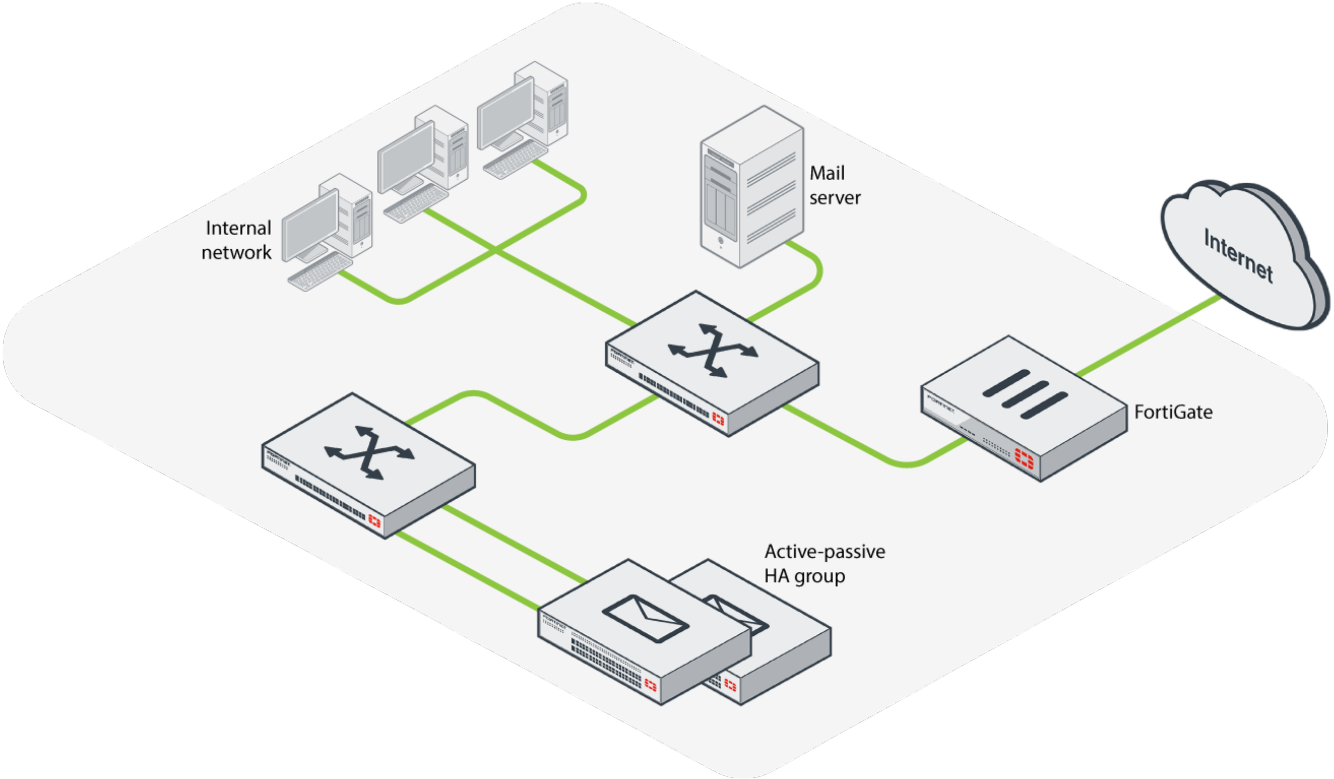
If the administrator account has somehow been deleted, enter the followng command to reset the FortiMail unit to its factory default configuration:

```
execute factoryreset
```

Getting started

This section contains information about installing and setting up FortiMail, as well common network configurations.

How to set up an active-passive HA in FortiMail



FortiMail supports two types of HA modes: active-passive HA pairs and config-only HA clusters. This recipe describes how to set up an active-passive HA.

Before beginning these procedures, be sure to register all FortiMail units in the HA group with Fortinet Support.

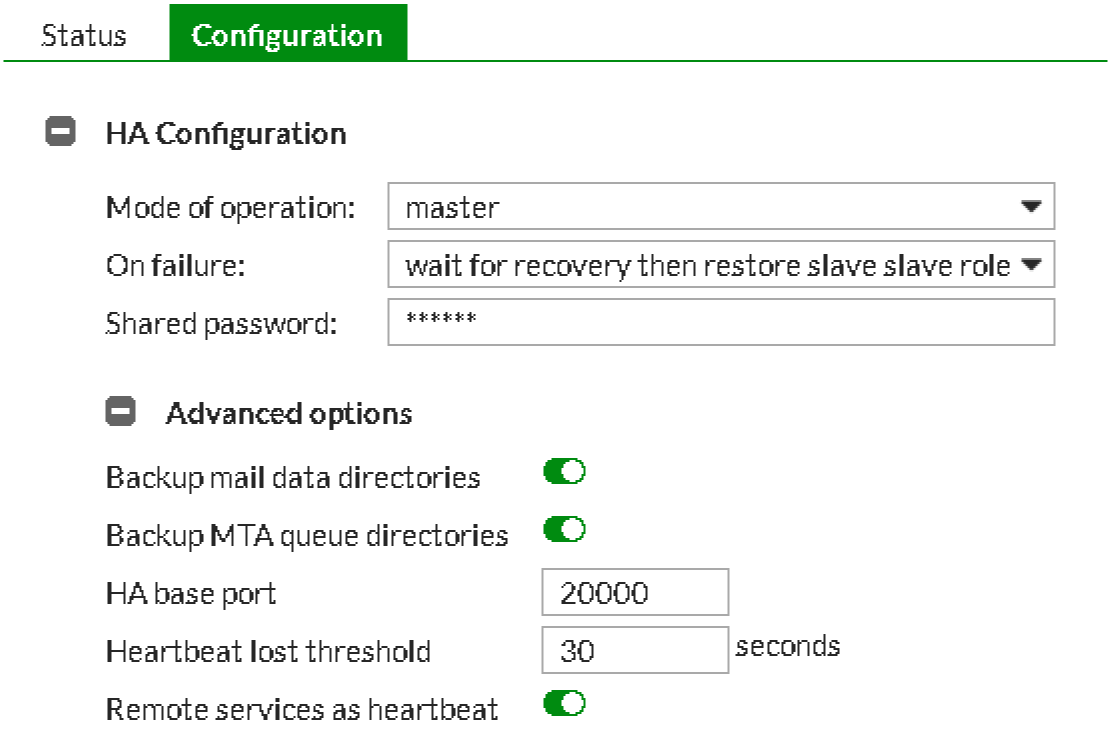
Configuring HA

1. Go to **System > High Availability > Configuration**.
2. Under **HA Configuration**, set **Mode of operation** to **primary** if the FortiMail unit is the primary unit in the active-passive group. Select **secondary** if the FortiMail unit is the secondary unit.
3. Set **On failure** to **wait for recovery then restore secondary role**. On recovery, the failed primary unit's effective HA mode of operation becomes **secondary**, and the secondary unit assumes the **primary** role.
4. Enter a **Shared password**. This password must be the same for both the primary and secondary units.
5. Expand **Advanced options** to configure backup options. Backup options only appear if you have selected either the **primary** or **secondary** mode of operation.
   Note that any backup settings configured are not synchronized across the active-passive group. To use this feature you must enable it on both primary and secondary units.
6. Enter an **HA base port** value (**20000** by default). This will be used for the heartbeat signal, and synchronization control, including data and configuration synchronization.

Note that, for active-passive HA groups, in addition to configuring the heartbeat, you can configure service-based failover and monitoring. For more information, see the FortiMail Administration Guide.

7. Set **Heartbeat lost threshold** to the total duration of time in seconds that the primary unit can be unresponsive before it triggers a failover, and the secondary unit assumes the role of the primary unit.
   Be sure not to set this value to too short a duration, as the secondary unit may falsely detect a failure during periods of high load.

   Conversely, if the failure detection time is too long, the primary unit could fail and a delay in detecting the failure could mean that email is delayed or lost. Decrease the failure detection time if email is delayed or lost because of an HA failover.
8. Enable **Remote services as heartbeat** to use remote services monitoring as a secondary HA heartbeat.
9. Click **Apply**.



Mode of operation: master

On failure: wait for recovery then restore slave slave role

Shared password: ******

Backup mail data directories ●

Backup MTA queue directories ●

HA base port 20000

Heartbeat lost threshold 30 seconds

Remote services as heartbeat ●

Configuring interface monitoring

Interface monitoring checks the local interfaces on the primary unit. If a malfunctioning interface is detected, a failover triggers.

1. Go to **System > High Availability > Configuration**.
2. Under **Interface**, select the port/interface you would like to configure and click **Edit**.
   Note that the interface IP address must be different from, but on the same subnet as, the IP address of the other heartbeat network interfaces of other members in the HA group.

Configuring alert emails in FortiMail

You might want your FortiMail unit to let you know when it has detected something. The **Alert Email** submenu lets you configure the FortiMail unit to email you when a specific type of event occurs. For example, you could have the unit alert you when it detects a virus.

To set up alerts we will have to configure both the alert email recipients and the events that trigger the unit to send a message.

Configuring alert recipients

Before the FortiMail unit can send alert email messages, we have to create a recipient list.

1. Go to **Log & Report > Alert Email > Configuration** and click **New**.
2. Enter the email address of a recipient and click **Create**.
3. Repeat this process to add all recipients required.

Configuring alert categories

Specify what events will cause your FortiMail unit to send an alert email message to the individuals you placed on the list previously.

1. Go to **Log & Report > Alert Email > Category**.
2. Enable one or more of the options available, such as **System events** to send an alert email when an important system event occurs.
3. When finished, click **Apply**.

Backing up and restoring mail data in FortiMail

FortiMail allows you to back up and restore all your existing mail data.

This recipe provides a detailed look at how to configure your FortiMail unit to back up and restore your mail data.

Mail data must be stored locally on the FortiMail hard disk in order for back up to work. If you store your mail data on a NAS device, you cannot back up your data. For more information on selecting storage devices, see "Selecting the mail data storage location" section in the FortiMail Administration Guide.

Configuring mailbox backup

Before you can initiate a backup or configure automatically scheduled backups, you must first enable backups and configure the backup media.

Before you can back up or restore your mail data, you must configure your FortiMail unit.

1. Go to **System > Maintenance > Mail Data**.
2. Expand **Status** and set a refresh rate from the **Automatically refresh interval** drop-down menu.
3. Under **Backup Options** click **Enable**.
4. Set the number of copies to fully backup.
5. Set either a full or incremental **Schedule**, depending on how often you wish to schedule backups.
6. Under **Device**, set **Protocol** to one of the following types of backup media:
   - **NFS**: A network file system (NFS) server.
   - **SMB/CIFS**: A Windows-style file share.
   - **SSH File System**: A server that supports secure shell (SSH) connections.
   - **External USB**: An external hard drive connected to the FortiMail unit's USB port.
   - **External USB (auto detect)**: An external disk connected to the FortiMail unit's USB port. Unlike the previous option, this option only creates a backup when you connect the USB disk, or when you manually initiate a backup using "Backing up and restoring the mailboxes" on page 299, rather than according to a schedule.
   - **iSCSI Server**: An Internet SCSI (Small Computer System Interface), also called iSCSI server.
7. Set **Hostname/IP address** to the IP address or FQDN of the NFS, Windows, SSH, or iSCSI server.
8. Set **Port** to the TCP port number on which the backup server listens for connections.
9. Set **Directory** to the folder path of the backup server where the FortiMail unit stores the mailbox backups, such as: */home/fortimail/mailboxbackups*.
10. Depending on the protocol you select, the following options are available:
    - **Share**: Enter the folder path of the backup server where the FortiMail unit stores the mailbox backups.
    - **Encryption key**: Enter the key used to encrypt data stored on the backup media. Valid key lengths are between six and 64 single-byte characters.
    - **iSCSI ID**: Enter the iSCSI identifier in the format expected by the iSCSI server, such as an iSCSI Qualified Name (IQN), Extended Unique Identifier (EUI), or T11 Network Address Authority (NAA).
11. Make sure to click Apply when finished configuring the **Backup Options** section.

Restoring from a backup

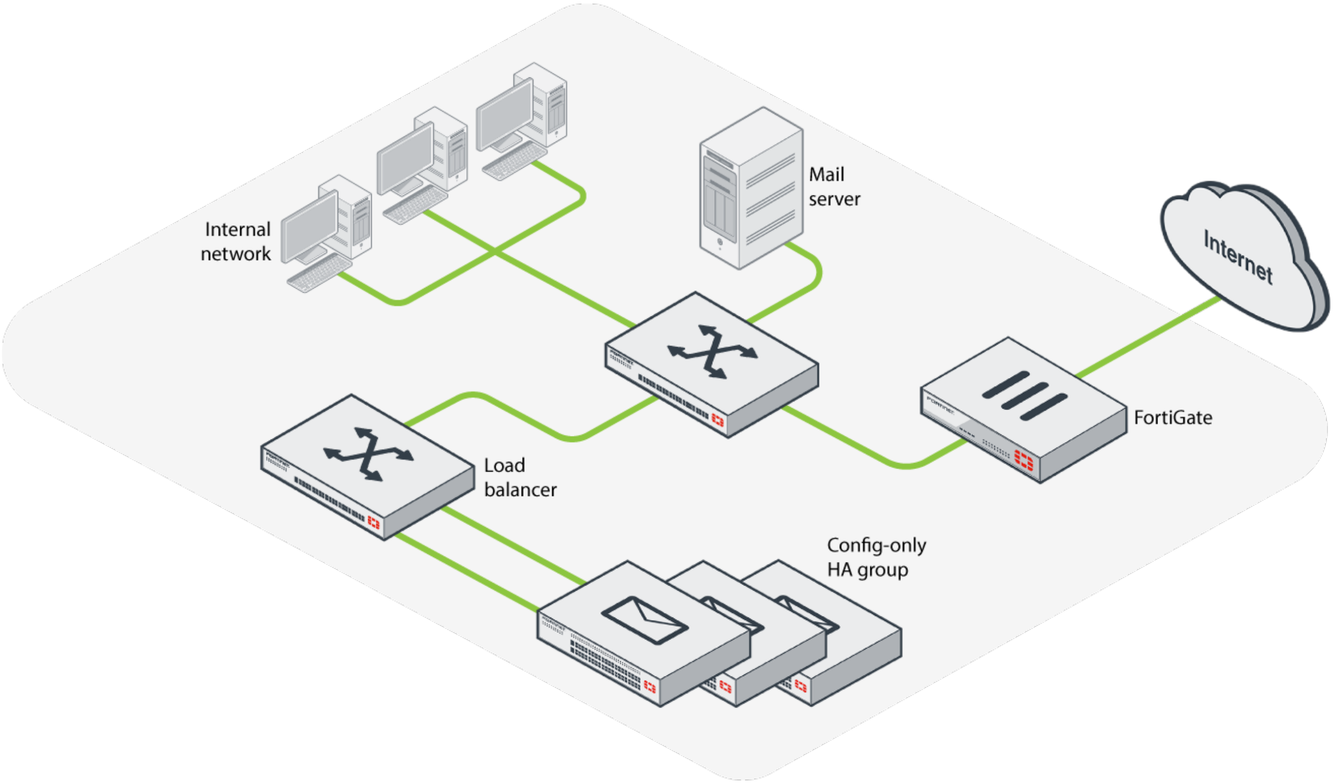
The **Restore Options** area of the Mail Data tab lets you selectively restore email users' mailboxes from mailbox backups.

1. Go to **System > Maintenance > Mail Data**.
2. Under **Restore Options**, select one of the following options:
   - **Created by this device**: Enable to restore mailboxes from backups identified by the current FQDN of this FortiMail unit.
   - **Created by**: Enable to restore mailboxes from backups identified by another FQDN or the FQDN of another FortiMail unit.
   - **For this domain**: Enable if you want to restore only the mailboxes of a specific protected domain. Once enabled, select the name of the protected domain from the drop-down menu. Optionally, enable **For this user** to restore only the mailbox of a specific email user.

   ⚠ Back up mailboxes before selecting the **Restore** button. Restoring mailboxes overwrites all mailboxes that currently exist.

3. Click **Restore** to restore mailboxes from the most recent full or incremental backup stored on the backup media. The time required to complete the restoration will vary depending on the size of the backup and the speed of your network connection.

How to set up a config-only HA in FortiMail



FortiMail supports two types of HA modes: active-passive HA pairs and config-only HA clusters. This recipe describes how to set up a config-only HA.

Config-only allows up to 25 FortiMail units to use an identical configuration, without synchronizing data and therefore operating as independent FortiMail units.

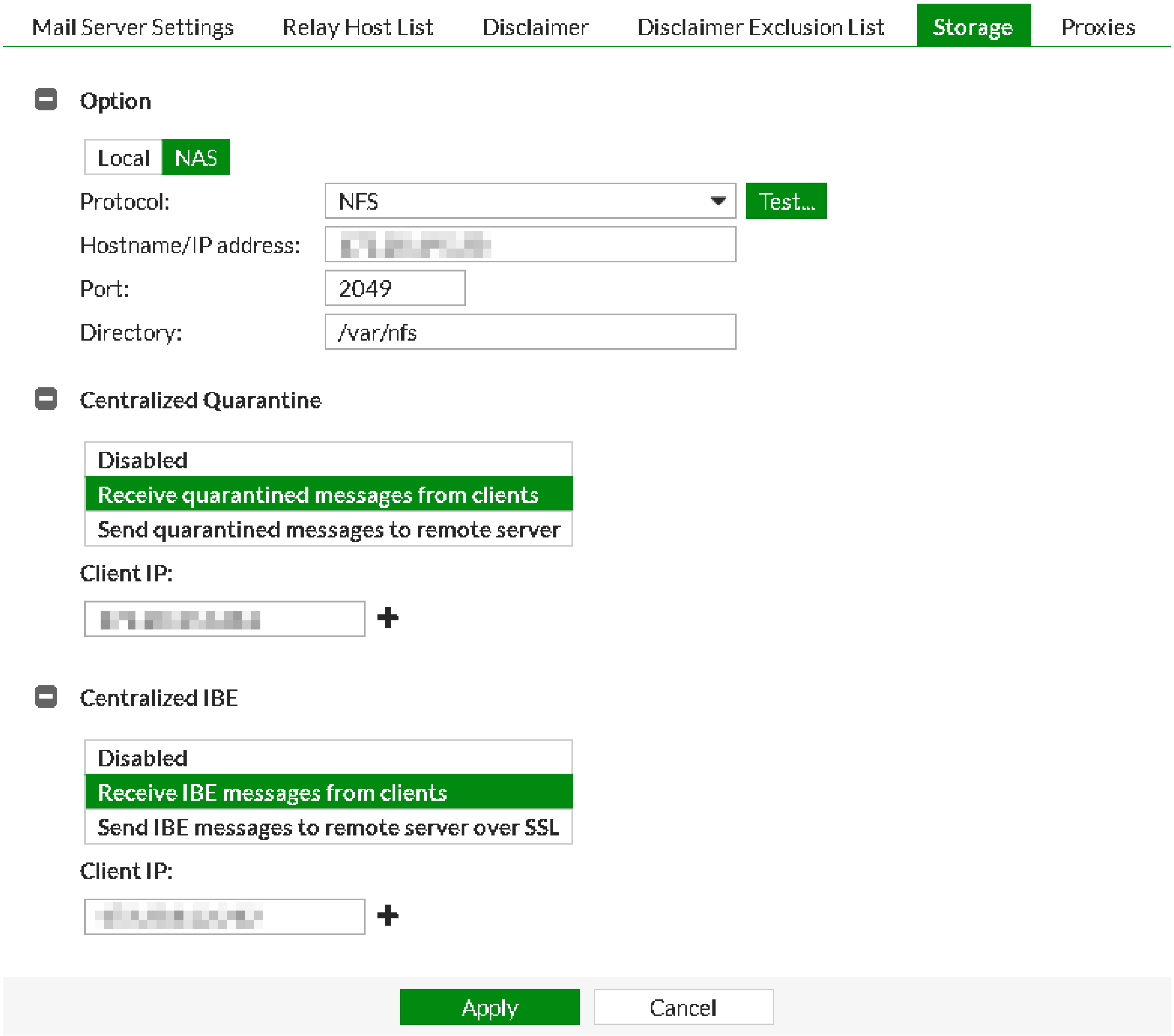
Before beginning these procedures, be sure to register all FortiMail units in the HA group with Fortinet Support.

Configuring mail data storage on a NAS server

Configure each member of the cluster to store mail data on a NAS server that supports NFS connections.

1. Go to **System > Mail Setting > Storage**.
2. Under **Option**, enable **NAS**.
3. Set **Protocol** to the type of NAS server: **NFS** or **iSCSI Server**.
4. Set the **Hostname/IP** address to the IP address of the NAS server.
5. Set the **Port** number to use, and enter a **Directory** path.
6. Configure the settings under **Centralized Quarantine** and/or **Centralized IBE** to determine whether the FortiMail unit will act as a centralized quarantine server or a centralized IBE mail storage server.

7. Click **Apply**.



Option

Local [✓ NAS]

Protocol: NFS

Hostname/IP address: [redacted]

Port: 2049

Directory: /var/nfs

Centralized Quarantine

Disabled
[✓ Receive quarantined messages from clients]
Send quarantined messages to remote server

Client IP: [redacted] +

Centralized IBE

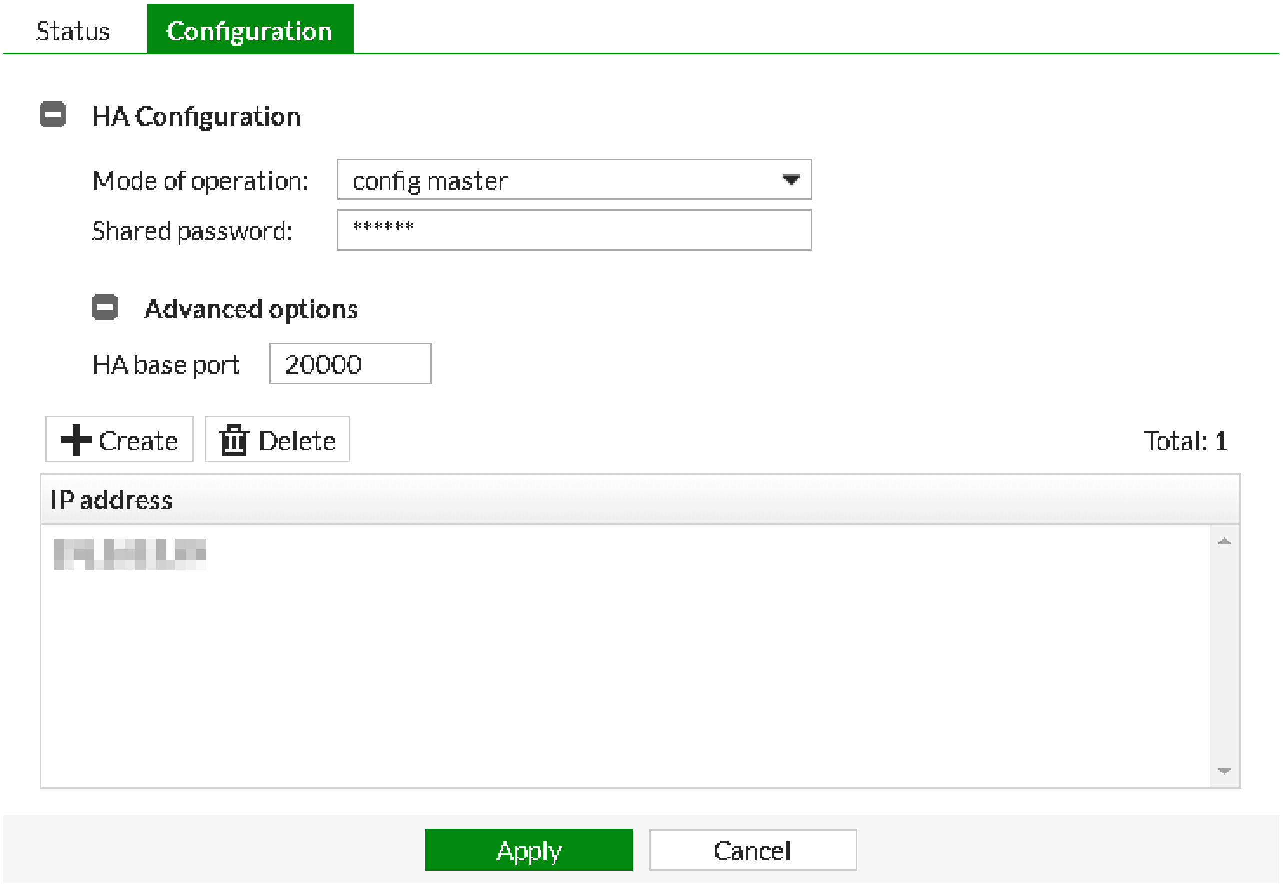
Disabled
[✓ Receive IBE messages from clients]
Send IBE messages to remote server over SSL

Client IP: [redacted] +

Configuring HA

1. Go to **System > High Availability > Configuration**.
2. Under **HA Configuration**, set **Mode of operation** to **config primary** if the FortiMail unit is the primary unit in the active-passive group. Select **config secondary** if the FortiMail unit is the secondary unit.
3. Enter a **Shared password**. This password must be the same for both the primary and secondary units.
4. Under **Advanced options**, set an **HA base port** value (**20000** by default). This will be used for the heartbeat signal, and synchronization control, including data and configuration synchronization.
5. Click **Create** and double-click the entry created. For the primary unit, enter the secondary unit's IP address. If you are configuring the secondary unit, enter the primary unit's IP address.

6. Click **Apply**.



HA Configuration

Mode of operation: config master

Shared password: ******

Advanced options

HA base port 20000

Total: 1

IP address
[redacted]

Custom replacement messages in FortiMail

Whenever your FortiMail unit detects a virus it replaces the attachment with a message that provides information on the virus and the source of the email. All messages received by your unit are customizable. This recipe guides you through the process of customizing your replacement messages.

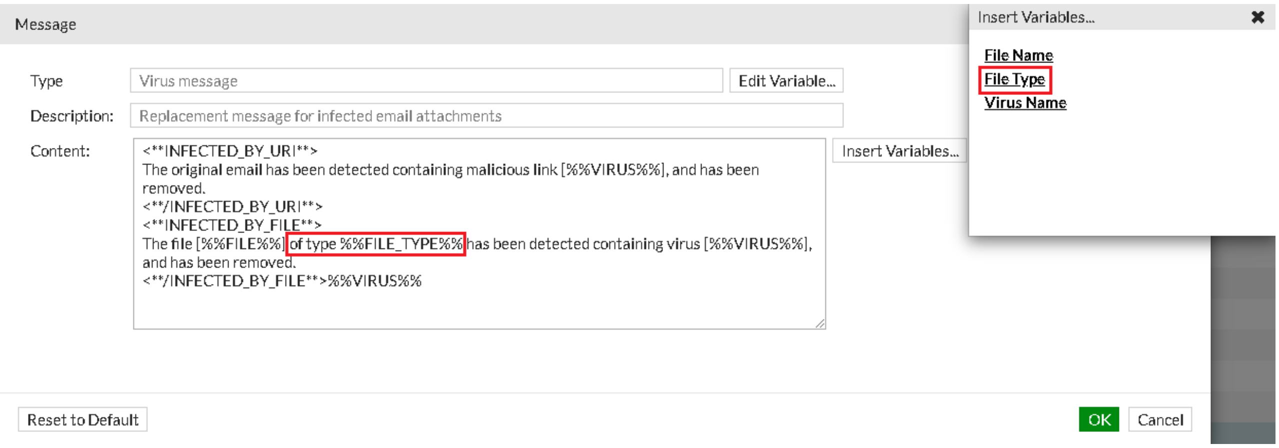
Configuring a custom message

Before you configure your custom message, you may create new variables to insert into your custom message. Typically, these variables represent messages that you will frequently use.

There is a substantial list of variables available to use. See the Creating variables section in the FortiMail Administration Guide.

For this example, no new variable is created. Instead, the predefined **File Type** variable is added into the content of the **Virus message** replacement message.

1. Go to **System > Customization > Custom Message**, select a replacement message (in this example, **Virus message** under **Replacement**), and click **Edit**.
   In this example, **Virus message** already has the file name (%%FILE%%) and virus name (%%VIRUS%%) variables in place.
2. Add the **File Type** variable (%%FILE_TYPE%%), so file types will be identified in any emails that are infected by a file.
   Enter the variable manually, or insert it by selecting it from the **Insert Variables** option.
3. Click **OK**.



Type: Virus message

Description: Replacement message for infected email attachments

Content:

```
<**INFECTED_BY_URI**>
The original email has been detected containing malicious link [%%VIRUS%%], and has been
removed.
<**/INFECTED_BY_URI**>
<**INFECTED_BY_FILE**>
The file [%%FILE%%] of type %%FILE_TYPE%% has been detected containing virus [%%VIRUS%%],
and has been removed.
<**/INFECTED_BY_FILE**>%%VIRUS%%
```

Deploying FortiMail Gateway mode

This recipe focuses on how to deploy FortiMail gateway mode when positioned within a private network and behind a firewall.

The FortiMail unit, the protected email server, and the email users' computers are positioned within a private network behind a firewall. The FortiMail unit, however, is located in the demilitarized zone (DMZ) of the firewall, separated from the local email users and the protected email server, which are located on the internal network of the firewall.

Remote email users' computers and external email servers are located on the Internet, outside of the network protected by the firewall. The FortiMail unit protects accounts for email addresses ending in "@example.com", which are hosted on the local email server.

Deploying FortiMail in gateway mode involves the following steps:

1. Connecting to FortiMail
2. Setting up FortiMail
3. Configuring DNS records
4. Configuring firewall policies
5. Configuring MUAs to use FortiMail
6. Testing the installation

Connecting to FortiMail

FortiMail port1's default IP address is 192.168.1.99. To access FortiMail's web UI, make sure you PC's IP address is on the same subnet as FortiMail (192.168.1.98).

1. Go to 192.168.1.99/admin.
2. Enter *admin* as the user name and no password by default.
3. Go to **Dashboard > Status**. In the **System Information** widget, set **Operation mode** to **Gateway**.

Setting up FortiMail

1. In the web-based manager of the FortiMail unit, click the administrator's options in the corner and go to **System > Wizard**.
   The Quick Start Wizard helps to configure some basic network and email settings when you load the interface for the first time.
2. Follow the onscreen instructions to configure the settings.
3. Once the Quick Start Wizard is finished, deploy the FortiMail unit into your network.

This setup uses the FortiMail default IP address. However, in most cases, you will need to change the IP address to deploy the unit into your network.

Configuring DNS records

Regardless of your private network topology, in order for external MTAs to deliver email to the FortiMail unit, you must configure the public MX record for each protected domain to indicate that the FortiMail unit is its email gateway.

For example, if the FQDN of the FortiMail unit is **fortimail.example.com**, and **example.com** is a protected domain, the MX record for **example.com** would be:

example.com IN MX 10 fortimail.example.com

A record must also exist to resolve the host name of the FortiMail unit into an IP address:

FortiMail IN A 10.10.10.1

If your FortiMail unit will relay outgoing email, you should also configure the public reverse DNS record. The public IP address of the FortiMail unit, or the virtual IP address on a firewall or router that maps to the private IP address of the FortiMail unit, should be globally resolvable into the FortiMail unit's FQDN. If it is not, reverse DNS lookups by external SMTP servers will fail.

For example, if the public network IP address of the FortiMail unit is 10.10.10.1, and fortimail.example.com is the FQDN of the FortiMail unit, a public DNS server's reverse DNS zone file for the 10.10.10.0/24 subnet might contain:

1 IN PTR fortimail.example.com

Configuring firewall policies

Whether or not the FortiMail unit is behind a firewall, such as a FortiGate unit, or in DMZ, you must configure a few firewall policies to allow the traffic.

For more information about how to create firewall policies, see your firewall documentation.

Configuring MUAs to use FortiMail

Configure the email clients of local and remote email users to use the FortiMail unit as their outgoing mail server (SMTP)/MTA. For local email users, this is the FortiMail IP address, 192.168.1.5. For remote email users, this is the virtual IP address on the wan1 network interface of the FortiGate unit that maps to the FortiMail unit, 10.10.10.1 or fortimail.example.com.

Also configure email clients to authenticate with the email user's user name and password for outgoing mail. The user name is the email user's entire email address, including the domain name portion, such as user1@example.com.

If you do not configure the email clients to authenticate, email destined for other email users in the protected domain may be accepted, but email outgoing to unprotected domains will be denied by the access control rule.

Testing the installation

To test the installation, send email messages by using the following test paths.

If you have problems with email delivery and receiving, check the following:

- Make sure the email clients use FortiMail as the incoming and outgoing email server.
- Make sure FortiMail can access the DNS servers.
- Make sure the Firewall policies allow SMTP traffic.

If you still have problems, contact Fortinet Technical Support.

Deploying FortiMail Server mode

FortiMail can act as a standalone SMTP mail server when running in Server mode. This recipe guides you through the process of setting up your FortiMail unit as a mail server.

Many of these steps require your FortiMail web interface to be running in Advanced mode.

Accessing Server mode

Before any advanced configuration, you must enable Server mode in the FortiMail web interface.

1. Ensure your computer’s IP address is on the same subnet as FortiMail’s default IP address (192.168.1.99).
2. Access the FortiMail web interface. FortiMail port1’s default IP address is 192.168.1.99. To access the FortiMail unit’s web UI, make sure your PC’s IP address is on the same subnet as FortiMail (for example, 192.168.1.98). Access this URL from a web browser: https://192.168.1.99/admin. The “/admin” portion of the URL is important.
3. Enter *admin* as the user name and no password by default.
4. Go to **Dashboard > Status**. In the **System Information** widget, set **Operation mode** to **Server**.
5. In the web-based manager of the FortiMail unit, click the administrator's options in the corner and go to **System > Wizard**.

   The Quick Start Wizard helps to configure some basic network and email settings when you load the interface for the first time.
6. Follow the onscreen instructions to configure the settings.

Configuring DNS records

In order for external MTAs to deliver email to the FortiMail unit, you must configure the public MX record for each protected domain to indicate that the FortiMail unit is its email server.

If your FortiMail unit will relay outgoing email, you should also configure the public reverse DNS record. The public IP address of the FortiMail unit, or the virtual IP address on a firewall or router that maps to the private IP address of the FortiMail unit, should be globally resolvable into the FortiMail unit’s FQDN. If it is not, reverse DNS lookups by external SMTP servers will fail.

For example, if the public network IP address of the FortiMail unit is 10.10.10.1, and fortimail.example.com is the FQDN of the FortiMail unit, a public DNS server’s reverse DNS zone file for the 10.10.10.0/24 subnet might contain:

1 IN PTR fortimail.example.com

Configuring firewall policies

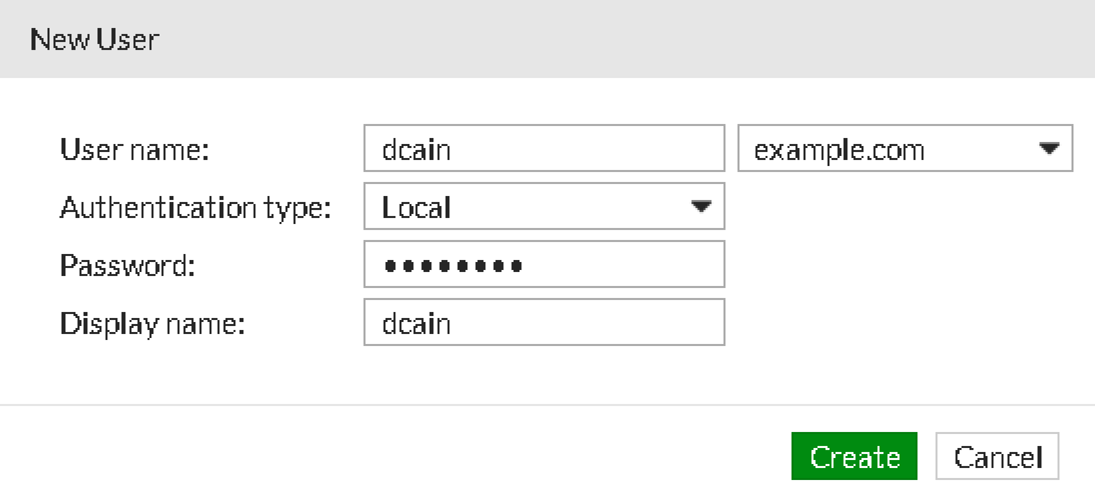
Whether or not the FortiMail unit is behind a firewall, such as a FortiGate unit, or in DMZ, you must configure a few firewall policies to allow the traffic.

For more information about how to create firewall policies, see your firewall documentation.

Adding email user accounts

Create an email user account for each protected domain to verify connectivity for the domain.

1. Go to **Domain & User > User > User**.
   Note that this is only available while the FortiMail unit is operating in **Server** mode.
2. Enter the **User name** of the email address that will be locally deliverable on the FortiMail unit (in the example, *dcain@example.com*).
3. Set your **Authentication type**.
4. Enter a **Password**.
5. Enter the **Display name** of the user as it should appear in an MUA.
6. Click **Create**.



New User

User name:	dcain	example.com
Authentication type:	Local	
Password:	••••••••	
Display name:	dcain	

Configuring MUAs to use for FortiMail

Configure the email clients of local and remote email users to use the FortiMail unit as their outgoing mail server (SMTP)/MTA. For local email users, this is the FortiMail IP address (192.168.1.5), for remote email users, this is the virtual IP address on the wan1 network interface of the FortiGate unit that maps to the FortiMail unit (10.10.10.1) or fortimail.example.com.

Configure email clients to authenticate with the email user’s user name and password for outgoing mail. The user name is the email user’s entire email address, including the domain name portion.

Testing the installation

Send emails from the local network and remotely to test successful SMTP and webmail POP3/IMAP connection.

Deploying FortiMail Transparent mode

This recipe details how to run a FortiMail unit in transparent mode.

Connecting to FortiMail from your PC

FortiMail port1’s default IP address is 192.168.1.99. To access FortiMail’s web UI, make sure you PC’s IP address is on the same subnet as FortiMail, for example, 192.168.1.98.

1. Access this URL from a web browser: *https://192.168.1.99/admin*
2. At the login page, enter *admin* as the user name and no password by default.
3. Go to **Dashboard > Status**. In the **System Information** widget, set **Operation mode** to **Transparent**.

Running the Quick Start Wizard

1. In the web-based manager of the FortiMail unit, click the administrator's options in the corner and go to **System > Wizard**.

   The Quick Start Wizard helps to configure some basic network and email settings when you load the interface for the first time.
2. Follow the onscreen instructions to configure the settings.

Configuring DNS records

When the FortiMail unit is operating in **Transparent** mode, in most cases, configuring DNS records for protected domain names is not required. Proper DNS records for your protected domain names are usually already in place.

However, you usually must configure public DNS records for the FortiMail unit itself, so that FortiMail can receive web connections, and send and receive email, for its own domain name. Dependent features include:

- delivery status notification (DSN) email
- spam reports
- email users' access to their per-recipient quarantined mail
- FortiMail administrators' access to the web UI by domain name
- alert email
- report generation notification email

You will also need to configure some transparent mode specific domain settings, in order to hide the presence of the FortiMail unit.

1. Go to **Domain & User > Domain > Domain** and edit a domain.
2. Expand **Transparent Mode Options**.
3. Set **This server is on** to the port to which the protected SMTP server is connected.
4. Enable **Hide the transparent box**, in order to preserve the IP address or domain name of the SMTP client.
5. Enable **Use this domain's SMTP server to deliver the mail**.

6. Click **OK**.
7. Go to **Profile > Session > Session** and click **New**, or edit an existing profile.
8. Optionally enable **Hide this box from the mail server**.

   Unless you have enabled both **Hide the transparent box** in each protected domain and **Hide this box from the mail server** in each session profile, the FortiMail unit is not fully transparent in SMTP sessions.

   In addition, unless you have enabled **Take precedence over recipient based policy match** in the IP-based policy, the **Hide the transparent box** option in the protected domain has precedence over this option, and may prevent it from applying to incoming email messages.

Configuring proxies

1. Go to **System > Network > Interface**, select **port1**, and click **Edit**.
2. Expand **SMTP Proxy**.
3. Set **Incoming connections** to **Drop**.
4. Set **Outgoing connections** to **Pass through**.
5. Enable **Local connections**.
6. Click **OK**.
7. Select **port2** and click **Edit**.
8. Set **Incoming connections** to **Proxy**.
9. Set **Outgoing connections** to **Drop**.
10. Disable **Local connections**.
11. Click **OK**.

Testing the installation

Send emails from the local network and remotely to test successful SMTP and webmail POP3/IMAP connection.

Encrypting confidential emails in FortiMail

You may want to send an email containing sensitive information, without the worry that someone could intercept the message and read the information.

Thankfully, your FortiMail unit can encrypt your messages. There are two ways you can encrypt your email messages:

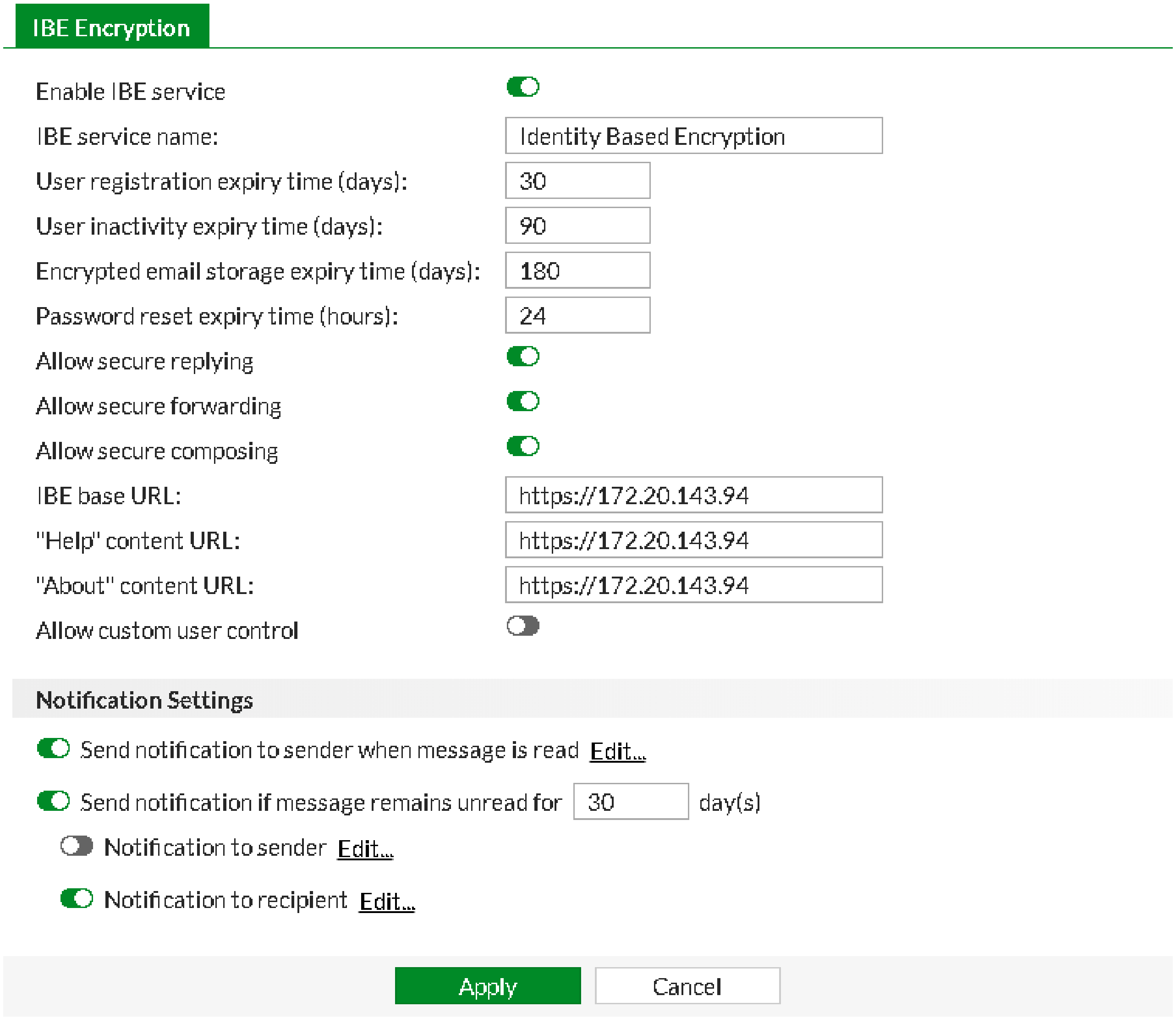
- **Content-based encryption**: The FortiMail unit can find key words in an email's subject header or message body to determine if a message should be encrypted. For example, if you add "Confidential" in your subject header, FortiMail will encrypt the email message.
- **Rule-based encryption**: The FortiMail unit encrypts all email sent from specific sources. For example, you could configure FortiMail to encrypt every email sent from the financial department.

This recipe covers content-based encryption.

Enabling the IBE service

1. Go to **Encryption > IBE > IBE Encryption** and click **Enable IBE service**.
2. Configure the options as necessary.

3. Click **Apply**.



IBE Encryption

Enable IBE service	●
IBE service name:	Identity Based Encryption
User registration expiry time (days):	30
User inactivity expiry time (days):	90
Encrypted email storage expiry time (days):	180
Password reset expiry time (hours):	24
Allow secure replying	●
Allow secure forwarding	●
Allow secure composing	●
IBE base URL:	https://172.20.143.94
"Help" content URL:	https://172.20.143.94
"About" content URL:	https://172.20.143.94
Allow custom user control	○

Notification Settings

● Send notification to sender when message is read Edit...

● Send notification if message remains unread for 30 day(s)

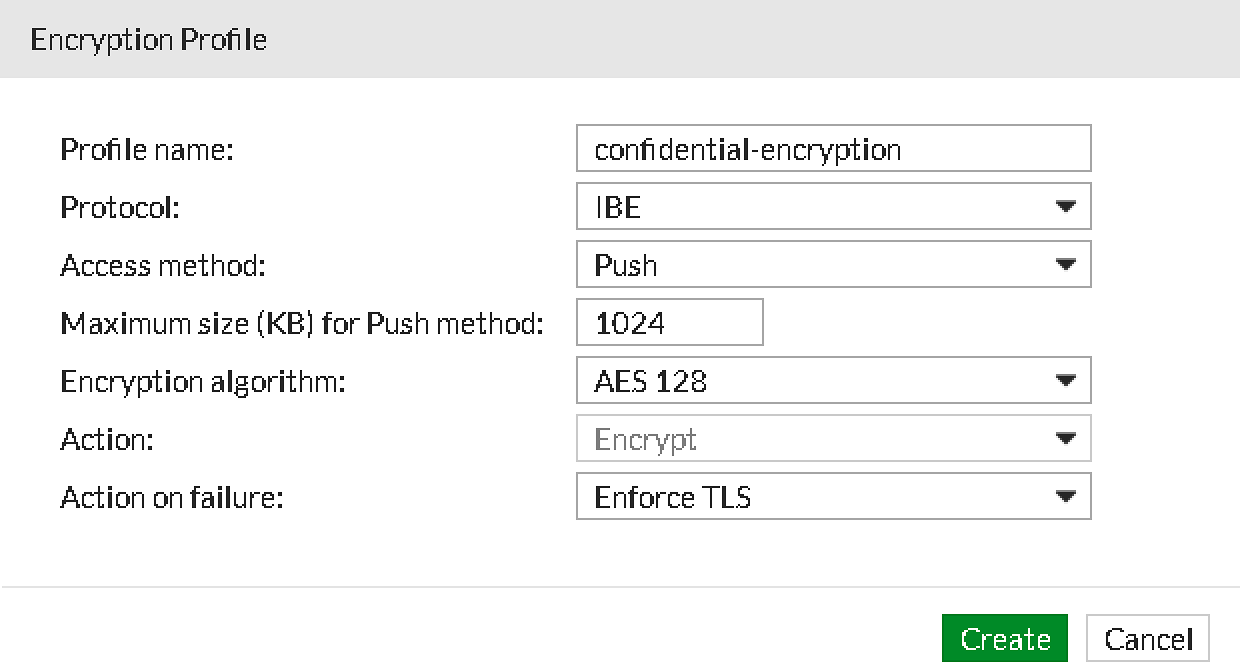
○ Notification to sender Edit...

● Notification to recipient Edit...

Configuring the encryption profile

1. Go to **Profile > Security > Encryption** and click **New**.
2. Enter a **Profile name**, and set **Protocol** to **IBE**.
3. Set **Access method** to **Push**, which sends a notification and secure email to the recipient for them to open the message. Unlike the **Pull** method, the FortiMail unit does not store the message.
4. Define a **Maximum size (KB) for Push method**.
   If the message exceeds the size limit, it will be delivered with the **Pull** method.
5. Set **Encryption algorithm** to the appropriate algorithm, and set **Action on failure** to **Enforce TLS**.

6. Click **Create**.



Encryption Profile

Profile name:	confidential-encryption
Protocol:	IBE
Access method:	Push
Maximum size (KB) for Push method:	1024
Encryption algorithm:	AES 128
Action:	Encrypt
Action on failure:	Enforce TLS

Configuring the content action profile

Content action profiles define the action taken by the FortiMail unit when it encounters an email containing a prohibited word or phrase. For more information on content action profiles, see the FortiMail Administration Guide.

1. Go to **Profile > Content > Action** and click **New**.
2. Enter a **Profile name**.
3. Enable **Final action** and select **Encrypt with profile** from the drop-down menu.
4. Set **Profile name** to the newly created encryption profile from the drop-down menu.
5. Configure the remaining settings as necessary.
6. Click **Create**.

Creating the dictionary profile

1. Go to **Profile > Dictionary > Dictionary** and click **New**.
2. Enter a **Name**.
3. Under **Dictionary Entries**, click **New**.
4. Enable both **Search header** and **Search body**.
5. Click **Create** and **Create** again.

Configuring the content profile

1. Go to **Profile > Content > Content** and click **New**.
2. Under **Content Monitor and Filtering** click **New**.
3. Click **Enable**.
4. Set **Dictionary** to the newly created dictionary profile from the drop-down menu.
5. Set **Minimum score** to the number of times that an email must match the dictionary profile before it receives the action configured in **Actions**.
6. Set **Actions** to the newly created action.
7. Click **Create**.

Configuring policies

Depending on whose email you want to encrypt, you can use either the IP-based or recipient-based policies. For example, if you want to apply encryption to everyone’s outbound email in the whole company, go to **Policy > Recipient Policy > Outbound** and create a recipient-based policy that uses a **Sender Pattern** of ***@example.com**.

How to encrypt emails sent from a designated source in FortiMail

You want to send emails containing sensitive information, but you're afraid that someone could intercept the message and read the information.

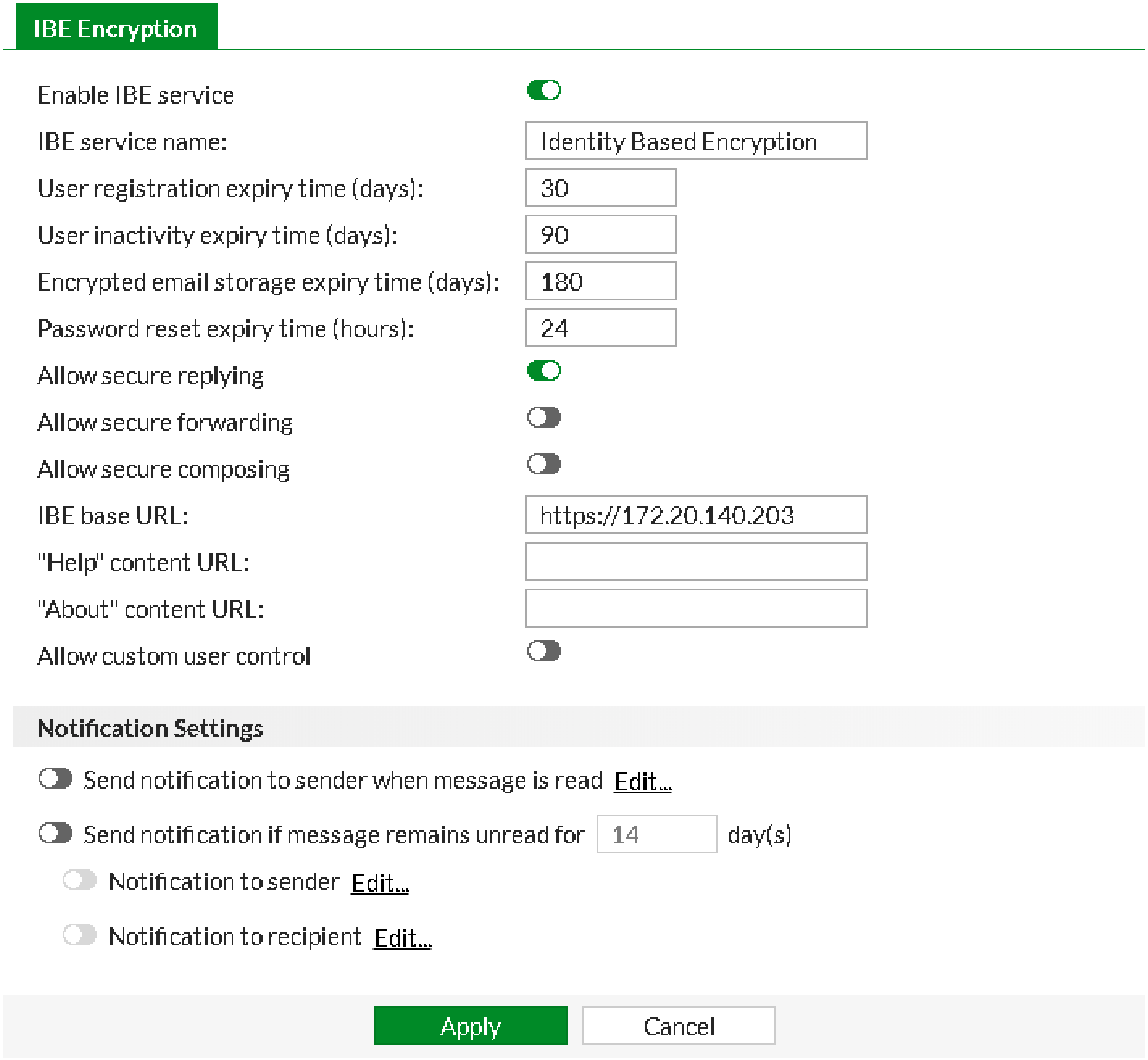
Thankfully, your FortiMail unit can encrypt all email messages sent from a designated source. For example, you could configure your FortiMail unit to encrypt every email sent from your financial department.

- **Content-based encryption**: The FortiMail unit can find key words in an email's subject header or message body to determine if a message should be encrypted. For example, if you add "Confidential" in your subject header, FortiMail will encrypt the email message.
- **Rule-based encryption**: The FortiMail unit encrypts all email sent from specific sources. For example, you could configure FortiMail to encrypt every email sent from the financial department.

Both of these methods are considered identity-based encryption (IBE). This recipe covers rule-based encryption.

Enabling the IBE services

1. Go to **Encryption > IBE > IBE Encryption**.
2. Click **Enable IBE service**.
3. Define the number of days that the secure mail recipient has to register on the FortiMail unit, the number of days the secure mail recipient can access the FortiMail unit without registration, and the number of days that the secured mail will be saved on the FortiMail unit.
4. Define the password reset expiry time in hours. This is for the recipients who have forgotten their login passwords and request for new ones.
5. Set **IBE base URL** to the the FortiMail unit URL that the mail recipient can use to register or authenticate and access the secure mail.
6. Configure the remaining settings as required, and click **Apply**.



IBE Encryption

Enable IBE service	●
IBE service name:	Identity Based Encryption
User registration expiry time (days):	30
User inactivity expiry time (days):	90
Encrypted email storage expiry time (days):	180
Password reset expiry time (hours):	24
Allow secure replying	●
Allow secure forwarding	○
Allow secure composing	○
IBE base URL:	https://172.20.140.203
"Help" content URL:	
"About" content URL:	
Allow custom user control	○

Notification Settings

○ Send notification to sender when message is read Edit...

○ Send notification if message remains unread for 14 day(s)

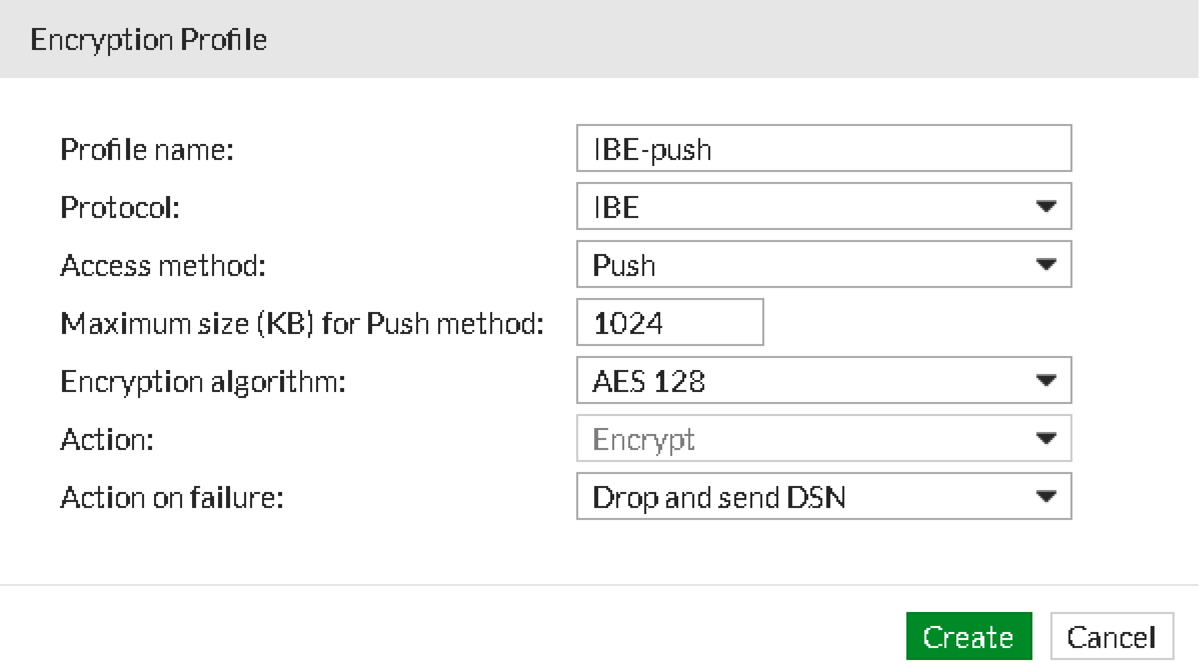
○ Notification to sender Edit...

○ Notification to recipient Edit...

Configuring the encryption profile

1. Go to **Profile > Security > Encryption** and click **New**.
2. Enter a **Profile name**.
3. Set **Protocol** to **IBE**.
4. Set **Access method** to one of the following:
   - **Push** sends a notification and secure mail to the recipient who needs to go to the FortiMail unit to open the message. The FortiMail unit does not store the message.
   - **Pull** sends just a notification to the recipient who needs to go to the FortiMail unit to open the message. The FortiMail unit stores the message.

5. Set **Maximum size (KB) for Push method** to the maximum message size of the secure mail delivered to the recipient.
   If the message exceeds the size limit, it will be delivered with the **Pull** method.
6. Assign an **Encryption algorithm**.
7. Set **Action on failure** to **Drop and send DSN**. When IBE is not available to send a secure mail to the recipient, a delivery status notification (DSN) email to the sender’s email address, indicating that the email is permanently undeliverable.
8. Click **Create**.



Encryption Profile

Profile name:	IBE-push
Protocol:	IBE
Access method:	Push
Maximum size (KB) for Push method:	1024
Encryption algorithm:	AES 128
Action:	Encrypt
Action on failure:	Drop and send DSN

Configuring delivery rules

Use the **Delivery** tab to view a list of delivery rules that apply to SMTP sessions being initiated by the FortiMail unit in order to deliver email.

1. Go to **Policy > Access Control > Delivery** and click **New**.
2. Click Enabled.

Installing FortiMail firmware using the CLI

When installing the latest firmware or older firmware you can use either the GUI or the CLI. This recipe shows how to install the firmware of your FortiMail unit using the CLI from a TFTP server.

This recipe assumes that the firmware image file you want to install is already copied to the root directory of the TFTP server.

Go to Fortinet Service & Support for the latest firmware. Whether you are upgrading or downgrading your firmware, it is strongly recommended to back up the configuration and mail data. For more information about configuration backups, see “Backup and Restore” in the FortiMail Administration Guide.

Firmware upgrade requires that you follow the supported firmware upgrade path, as FortiMail units running older firmware versions may not successfully install the latest firmware version. See the appropriate FortiMail Release Notes for the correct upgrade path.

Connecting the hardware

1. Connect your computer to the FortiMail unit's console port using an RJ-45 to DB-9 serial cable or a null-modem cable.
2. Initiate an connection from your computer to the CLI of the FortiMail unit and log in as an administrator.
   If this is the first time connecting to the FortiMail unit, the default account is `admin` with no password.
3. Connect port1 of the FortiMail unit directly to the same subnet as a TFTP server.

Installing the firmware

1. To verify connectivity to the TFTP server in the CLI, enter the following command:
   ```
   execute ping <tftp_ipv4>
   ```
   Where `<tftp_ipv4>` is the IP address of the TFTP server.
2. To download the firmware image from the TFTP server, enter the following command:
   ```
   execute restore image tftp <name_str> <tftp_ipv4>
   ```
   Where `<name_str>` is the file name of the firmware image.
3. A prompt will appear. Enter `y` to confirm the firmware install and upgrade.
   The FortiMail unit installs the firmware and restarts. This may take several minutes depending on the size of the file and the speed of your network connection.

   If you are downgrading the firmware to a previous version, the FortiMail unit reverts the configuration to default values for that version of the firmware. You must either reconfigure the FortiMail unit or restore a backup configuration file.
4. Once the FortiMail unit has finished restarting, clear your web browser cache and restart the browser to ensure it reloads the web UI.
5. To verify that the firmware version successfully installed, from the CLI, enter the following command:
   ```
   get system status
   ```

Installing firmware replaces the current FortiGuard AntiVirus definitions with those included with the newly installed firmware release. In addition to verifying the firmware, make sure that the **Virus DB** entry is updated too.

Reconnecting to the FortiMail unit after a downgrade

If you downgrade to a previous version, the FortiMail unit reverts to default settings, including the IP addresses of network interfaces through which you connect to the FortiMail GUI and CLI.

If this occurs, you can reconnect again using the CLI.

1. Connect your computer to the FortiMail unit's console port using an RJ-45 to DB-9 serial cable or a null-modem cable.
2. Start HyperTerminal, or PuTTY, and enter a name for the serial connection (for example, **COM1**).
3. Set the following port settings:
   - **Speed (baud)**: 9600 (bits per second)
   - **Data bits**: 8
   - **Stop bits**: 1
   - **Parity**: None
   - **Flow control**: None
4. Press **Enter** or click **Open** to connect to the FortiMail CLI and log in as the default admin account (`admin` with no password).
5. Once logged in, enter the following command to reinstate the network interface IP address for `port1` and allow administrative access to the FortiMail unit through the GUI and CLI:
```
config system interface
   edit port1
      set ip <ip/netmask>
      set allowaccess ping https ssh
end
```
   Where `<ip/netmask>` is the IP address and netmask of the network interface, such as `192.168.1.10/24`.

Restoring the configuration

If you want to restore a backup of an older configuration from your PC, use the following steps in the FortiMail web UI.

1. Go to **Dashboard > Status**.
2. In the **System Information** widget, under **System configuration**, click **Restore**.
3. Navigate to and select your backup configuration file.
4. Click **Open**.
5. Follow the remaining prompts to confirm the restoration.

Configuring and viewing FortiMail log messages

This recipe shows how to store log messages locally on the hard disk of the FortiMail unit, and how to create backup copies. To ensure that the local hard disk has sufficient space for new log messages, it is recommended to regularly download backup copies of the oldest log files to your computer and then delete them from the FortiMail unit.

Log messages can be stored both locally and remotely. To store log files remotely, see “Configuring logging to a Syslog server or FortiAnalyzer unit” in the FortiMail Administrator Guide.

Enabling and configuring log settings

To access your log messages on the FortiMail GUI, your administrator account’s **Domain** must be set to **System**. This is configured under **System > Administrator > Administrator**.

In addition, the administrator's access profile must have **Read Only** or **Read-Write** permissions set in the **Others** category. This is configured under **System > Administrator > Admin Profile**.

To enable and configure logging to the local hard disk:

1. Go to **Log & Report > Log Setting > Local** and click **Enable**.
   The FortiMail unit will rotate the current log and start a new log file depending on whether the log file reaches a certain file size in MB or age in days first.
2. Set **Log file size** to the file size limit (100 MB by default).
3. Set **Log time** to the file age limit (45 days by default), and the hour of the day that the file rotation should occur.
4. Set **Log level** to the severity-level that a log message must equal or exceed for it to be recorded.
   Although set to **Information** by default, avoid using low-level severities (such as **Information** or **Notification**), as this can lead to an excessive logging frequency, which can be detrimental to the system's longevity.
5. Set **Log retention period** to the number of days that a log will be kept before it is deleted (up to a maximum of 1461 days, or approximately four years). 0 means no limit.
6. Set **Log options** when disk is full to the appropriate action: **Overwrite** to delete the oldest log file in order to free disk space and store the new log message, or **Do not log** to discard all new log messages.
7. Under **Logging Policy Configuration**, enable the types of events to be included in the generated logs. Expand **System Event** and **Mail Event** for more granular control.
8. Click **Apply**.

Monitoring and downloading log messages

Once you have configured your log settings, you can view the generated reports from the log data.

1. Go to **Monitor > Log**, and click the corresponding tab according to which type of log you want to view: **System Event**, **Mail Event**, **AntiVirus**, **AntiSpam**, or **Encryption**.
2. Double-click an entry to view its log details.
3. To download a backup of a log report, click **List** from any of the log monitor tabs.

All the log entries are compiled into log reports, each with a **Start Time** and **End Time** in accordance to your log settings defined earlier.

4. Select a log report and click **Download**. Reports can be downloaded in the following formats:
   - **Normal Format**: A log file that can be viewed with a plain text editor such as Microsoft Notepad.
   - **CSV Format**: A comma-separated value (.csv) file that can be viewed in a spreadsheet application such as Microsoft Excel.
   - **Compressed Format**: A log file like the **Normal Format** but compressed as a .gz archive.

Real-time scanning of Microsoft 365 email in FortiMail

In this recipe, you'll configure FortiMail to protect Microsoft 365 email users by scanning incoming email right after the email reaches their mailbox.

Once you have linked your Microsoft 365 account to the FortiMail unit, you will enable and configure real-time scanning. You will then simulate a spam email that real-time scanning will identify and take the appropriate action.

The Microsoft 365 real-time scan feature requires the following:

- A valid CA signed certificate
- The FortiMail unit must be reachable by hostname (not IP address)

Real-time scanning allows you to apply security profiles and their actions to only those emails that match certain criteria specified in a real-time scan policy. These criteria are based on source, sender, and recipient information.

You can also optimize the efficiency of real-time scanning by enabling the `hide-email-on-arrival` CLI command. This feature restricts users from receiving and opening potentially dangerous emails by first subjecting the email to real-time scanning. Only when the email is deemed safe is it then moved to the users mailbox.

Retrieving your Microsoft 365 account information

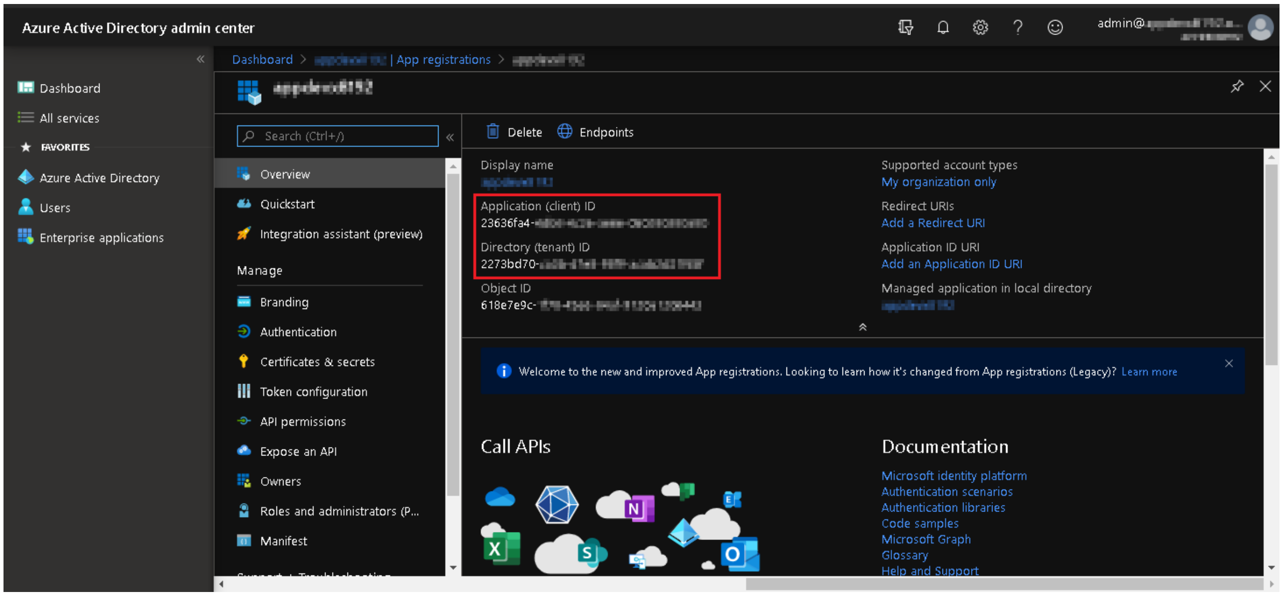
Adding your Microsoft 365 account in FortiMail requires that you provide your **Tenant ID**, **Application ID**, and **Application Secret**. At the time of writing, these are located in various areas on the Microsoft 365 portal.

Note that for the purpose of this recipe, the default domain attached to your Microsoft 365 account is used. This domain is set up to have DNS records managed by Microsoft 365, and is already configured to be used with Microsoft 365 services.

To locate the Tenant ID and Application ID:

Note that after acquiring the **Tenant ID** and **Application ID**, you must also grant consent permissions for the admin.

1. Log in to Microsoft 365.
2. From the landing page, click *Admin*.
3. From the left-hand menu, click *Show all* > *Admin centers* > *Azure Active Directory*.
4. Under *Favorites*, click *Azure Active Directory*.
5. Under *Manage*, click *App registrations*.
   The *Overview* of your application automatically appears on the screen, displaying your *Application (client) ID* and *Directory (tenant) ID*. These are required later and serve as the *Application ID* and *Tenant ID* (respectively) when adding the account in FortiMail.



Display name
[redacted]

Application (client) ID
23636fa4-[redacted]

Directory (tenant) ID
2273bd70-[redacted]

Object ID
618e7e9c-[redacted]

Supported account types
My organization only

Redirect URIs
Add a Redirect URI

Application ID URI
Add an Application ID URI

Managed application in local directory
[redacted]

Welcome to the new and improved App registrations. Looking to learn how it's changed from App registrations (Legacy)? Learn more

Call APIs

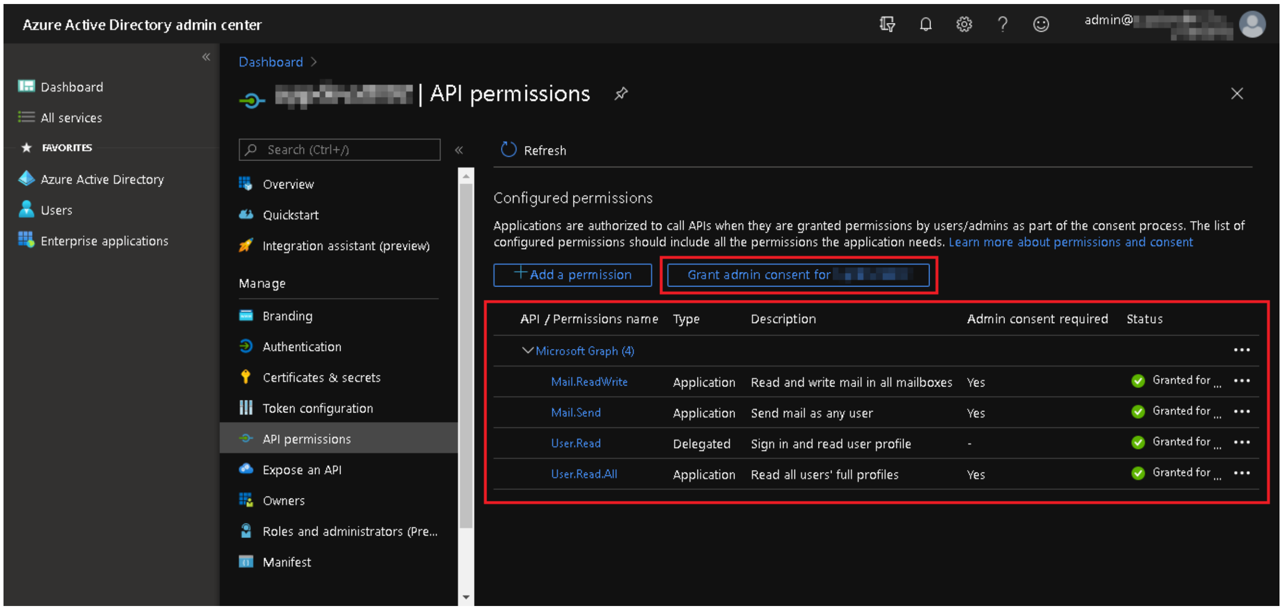
Documentation

Microsoft identity platform
Authentication scenarios
Authentication libraries
Code samples
Microsoft Graph
Glossary
Help and Support

6. Copy the values of both IDs and paste them to a text-editor for the time being.
7. From the application, under *Manage*, click *API permissions*.
8. Click *Add a permission* > *Microsoft Graph* > *Application permissions*.
9. Add the following permissions:
   - *User.Read.All*
   - *Mail.ReadWrite*
   - *Mail.Send*

   Note that *User.Read* is added by default.

10. Click *Grant admin consent for admin*.



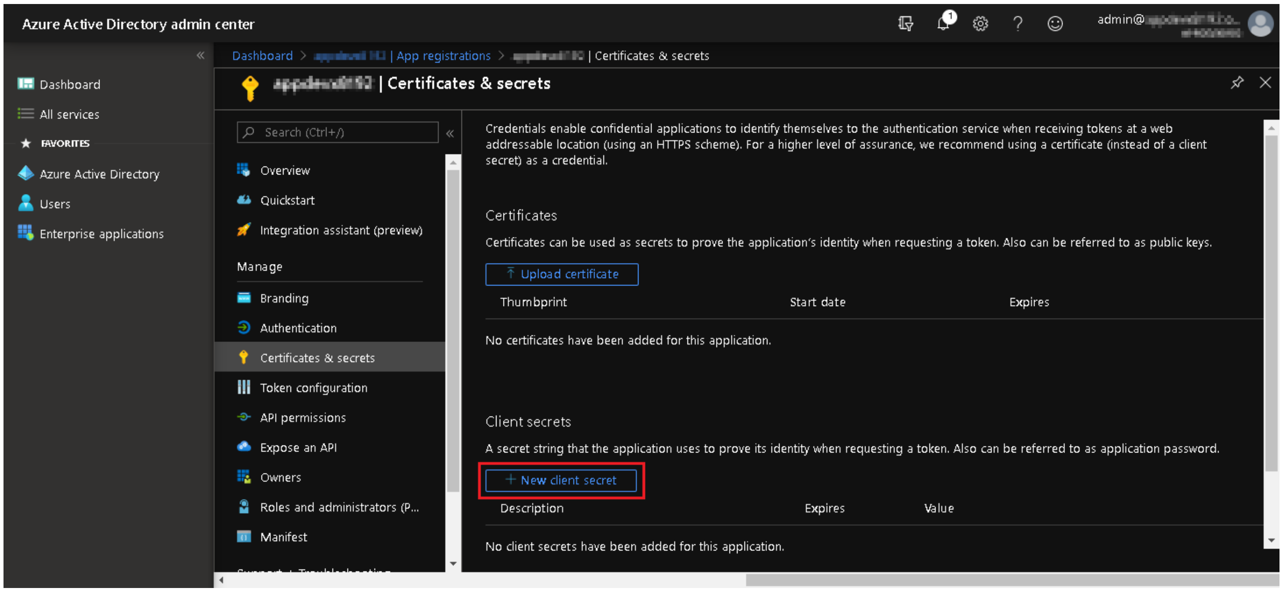
Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. Learn more about permissions and consent

API / Permissions name	Type	Description	Admin consent required	Status
Microsoft Graph (4)				
Mail.ReadWrite	Application	Read and write mail in all mailboxes	Yes	✓ Granted for ...
Mail.Send	Application	Send mail as any user	Yes	✓ Granted for ...
User.Read	Delegated	Sign in and read user profile	-	✓ Granted for ...
User.Read.All	Application	Read all users' full profiles	Yes	✓ Granted for ...

To locate the Application Secret:

1. From the *Azure Active Directory*, under *Manage*, click *Certificates & secrets*.
2. Under *Client secrets*, click *New client secret*.



Azure Active Directory admin center

admin@[redacted]

Dashboard > [redacted] | App registrations > [redacted] | Certificates & secrets

[redacted] | Certificates & secrets

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Certificates

Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.

Thumbprint	Start date	Expires

No certificates have been added for this application.

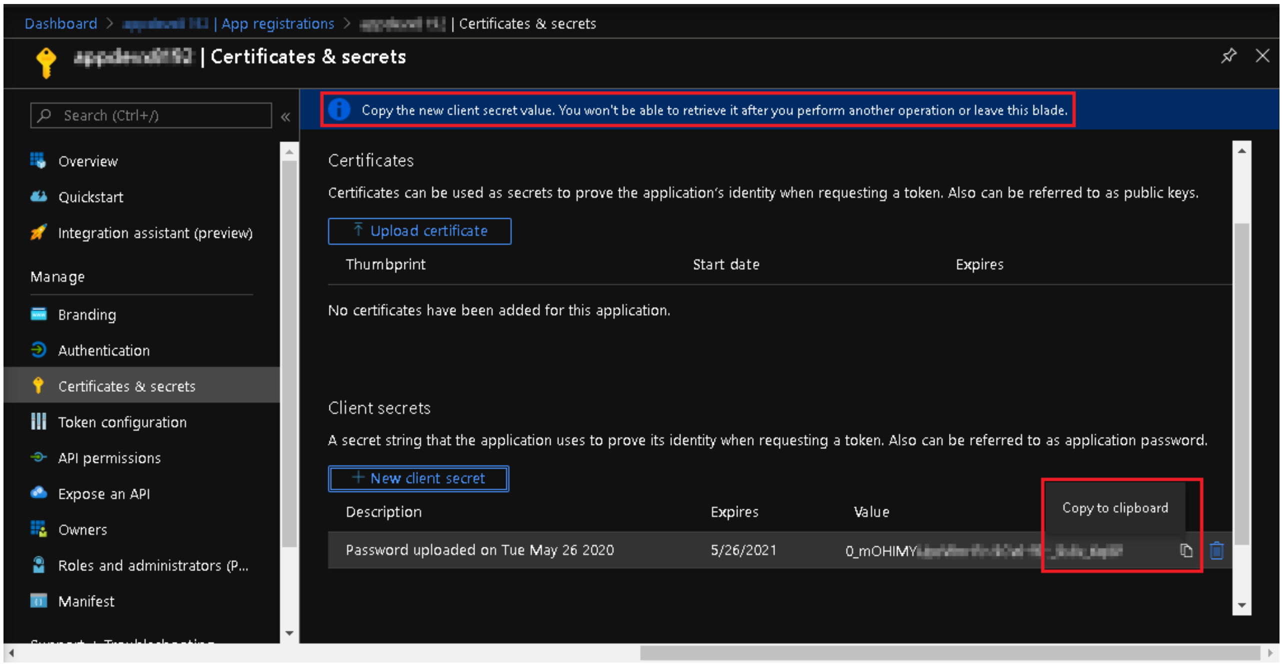
Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

Description	Expires	Value

No client secrets have been added for this application.

3. Enter an optional *Description*, select the appropriate expiration option, and click *Add*.
   Your new client secret is created. Note the warning stating that you **must** immediately copy this password, as it will not be retrievable after you perform another action or navigate away from this page.
4. Copy the value of the secret and paste it to the text-editor already holding the tenant and application ID.



Dashboard > [redacted] | App registrations > [redacted] | Certificates & secrets

[redacted] | Certificates & secrets

Copy the new client secret value. You won't be able to retrieve it after you perform another operation or leave this blade.

Certificates

Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.

Thumbprint	Start date	Expires

No certificates have been added for this application.

Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

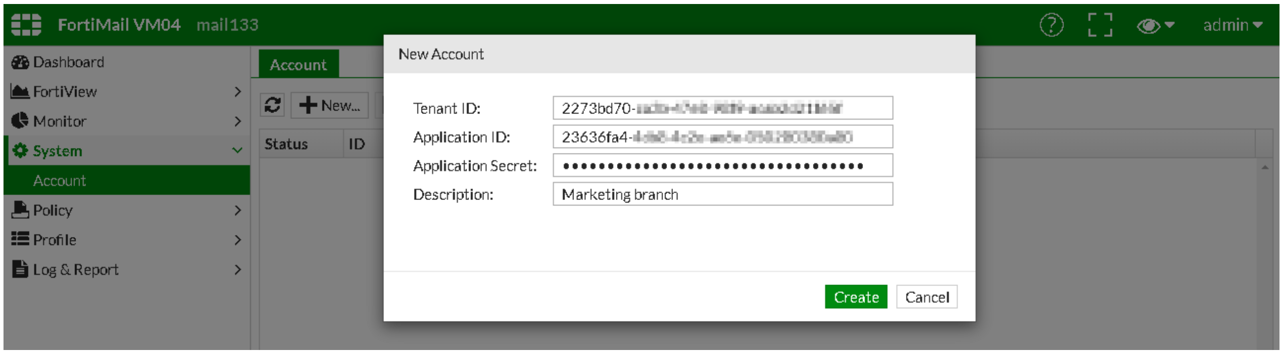
Description	Expires	Value
Password uploaded on Tue May 26 2020	5/26/2021	0_mOHIMY[redacted]

You now have all the information required to add your Microsoft 365 account in FortiMail.

Adding Microsoft 365 account in FortiMail

Now that you have all the necessary credentials, you must add your Microsoft 365 account in FortiMail to begin configuring real-time scanning of your emails.

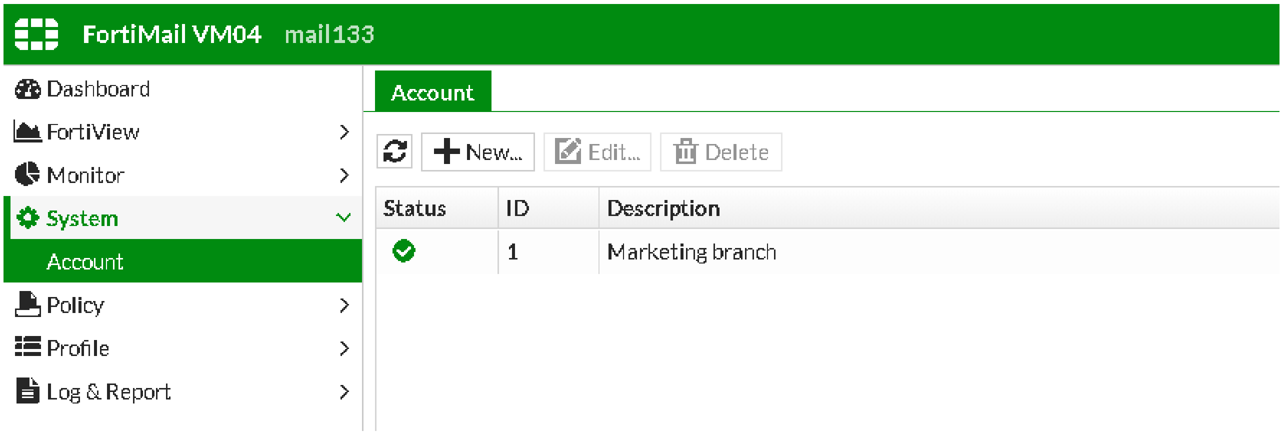
1. In FortiMail, go to *View* > *Microsoft 365 View*.
2. Go to *System* > *Account* > *Account* and click *New*.
3. Copy and paste your *Tenant ID*, *Application ID*, and *Application Secret* into the fields provided.
4. Click *Create*.



New Account

Tenant ID: 2273bd70-[redacted]
Application ID: 23636fa4-[redacted]
Application Secret: ••••••••••••••••••••••••••••••••
Description: Marketing branch

The account is successfully added to FortiMail, showing a green-status check mark.



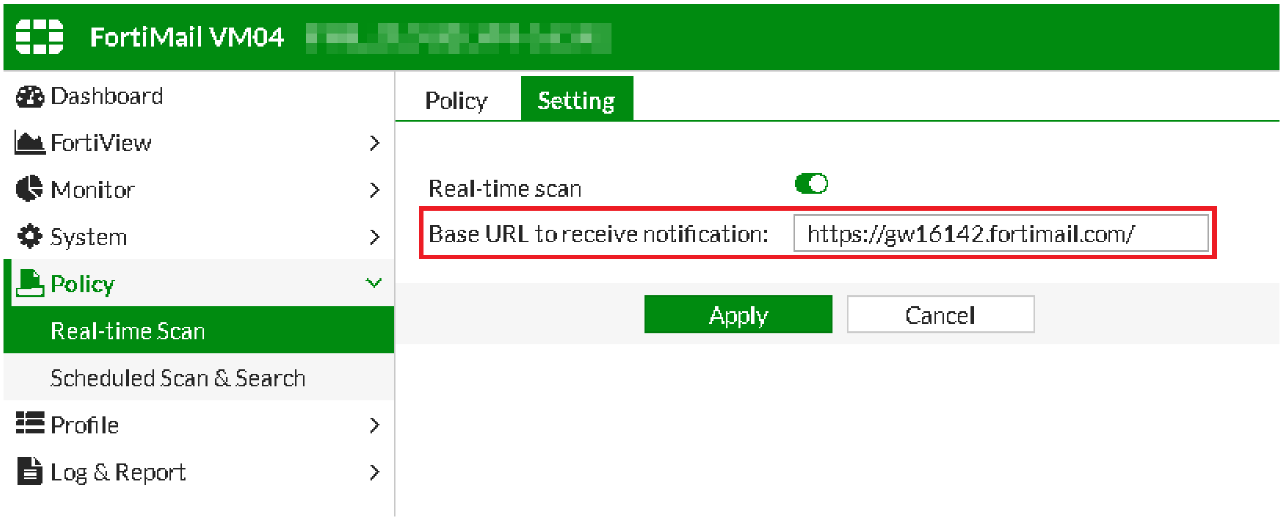
Status	ID	Description
✓	1	Marketing branch

Enabling real-time scanning

Before you can begin configuring real-time scan policies, you must first enable the feature, and define the base URL for the FortiMail unit to receive notifications from Microsoft 365.

1. Go to *View* > *Microsoft 365 View*.
2. Go to *Policy* > *Real-time Scan* > *Setting*.
3. Enable *Real-time scan*.
4. Enter a *Base URL to receive notification* in the following format:
   ```
   https://<host-name>.<local-domain-name>.com/
   ```
   Note that by default this should already be auto-populated, as per the mail server settings under *System* > *Mail*

Setting > *Mail Server Setting* from the *Advanced View* of the GUI.



Real-time scan: on

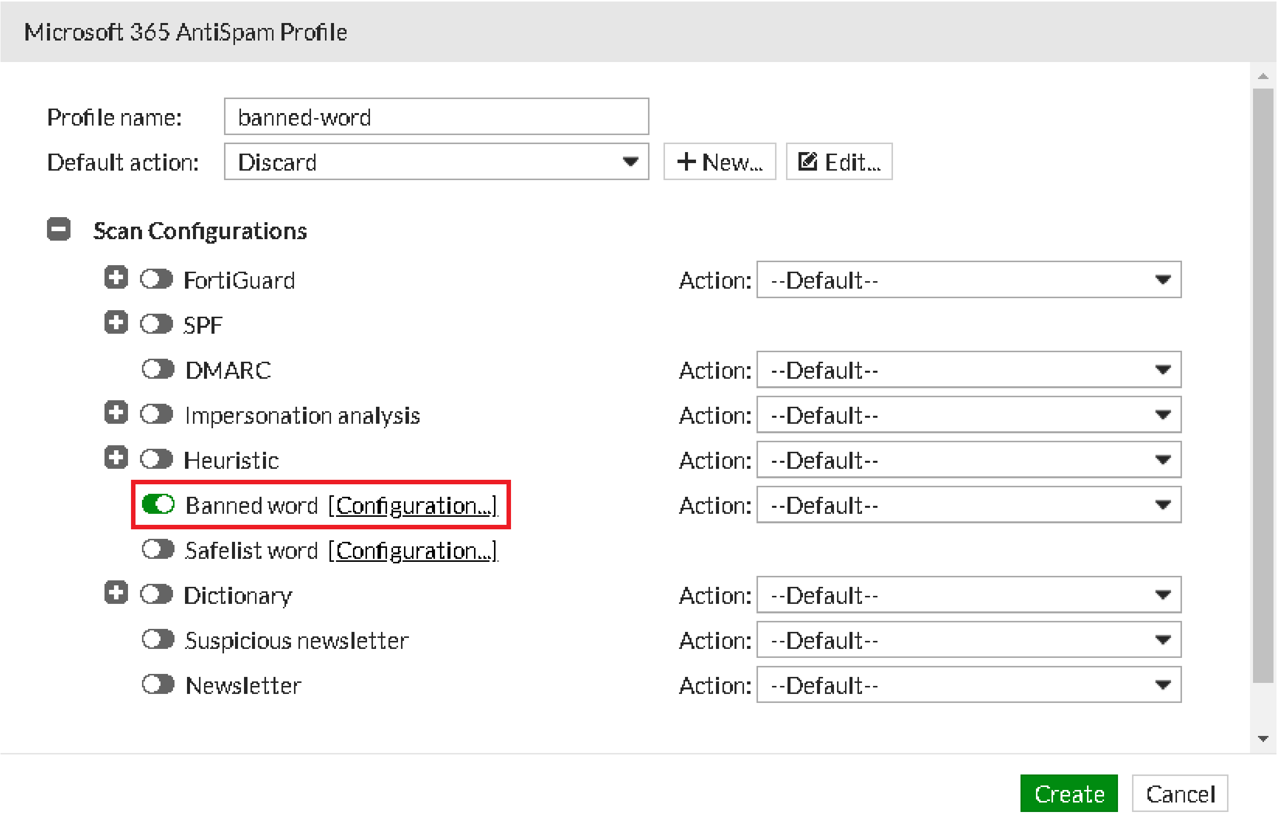
Base URL to receive notification: https://gw16142.fortimail.com/

Configuring real-time scan policy

To test the real-time scan policy, in this example, you will create an antispam profile configured to discard any reference to a banned word string. You will assign the antispam profile to a real-time scan policy. All emails matching the search criteria of the profile and policy will be discarded.

To configure the antispam profile:

1. Go to *View* > *Microsoft 365 View*.
2. Go to *Profile* > *AntiSpam* > *AntiSpam* and click *New*.
3. Enter a *Profile name* and set *Default action* to an action profile set to *Discard*.
4. Under *Scan Configurations*, enable *Banned word* and click *Configuration*.



Microsoft 365 AntiSpam Profile

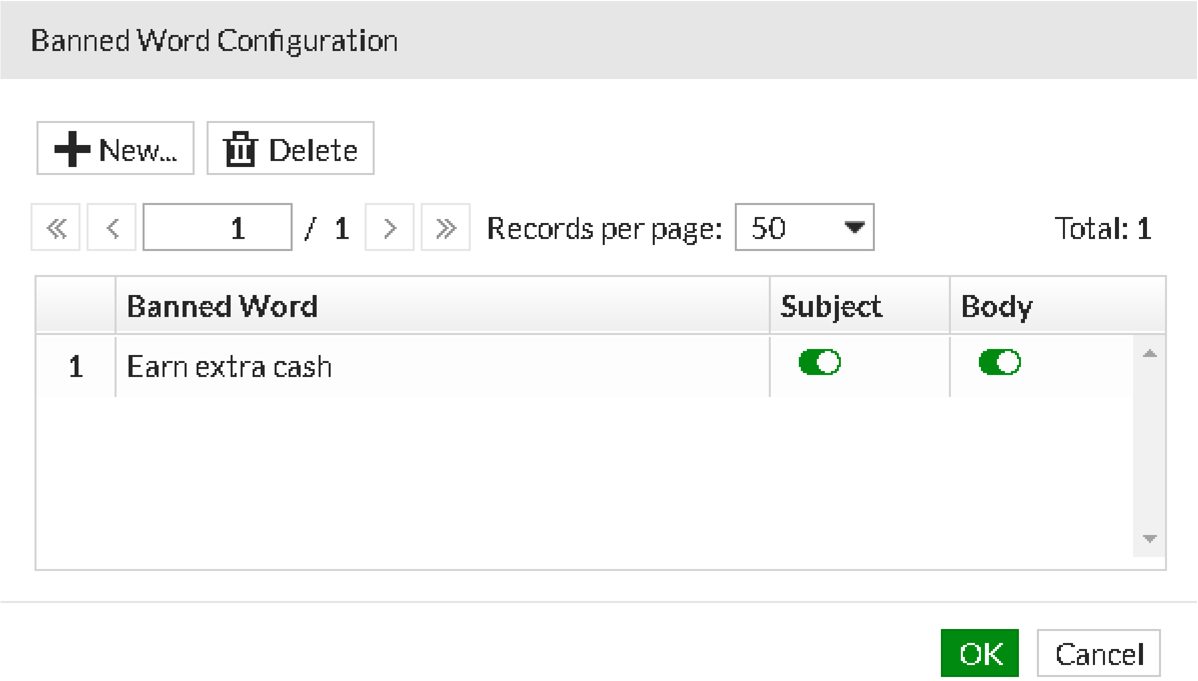
Profile name: banned-word

Default action: Discard

Scan Configurations

○ FortiGuard	Action: --Default--
○ SPF	
○ DMARC	Action: --Default--
○ Impersonation analysis	Action: --Default--
○ Heuristic	Action: --Default--
● Banned word [Configuration...]	Action: --Default--
○ Safelist word [Configuration...]	
○ Dictionary	Action: --Default--
○ Suspicious newsletter	Action: --Default--
○ Newsletter	Action: --Default--

5. Click *New*, and enter a word or string you wish to ban.
By default, both the email's *Subject* header and *Body* will be searched.



Banned Word Configuration

1 / 1 Records per page: 50 Total: 1

	Banned Word	Subject	Body
1	Earn extra cash	●	●

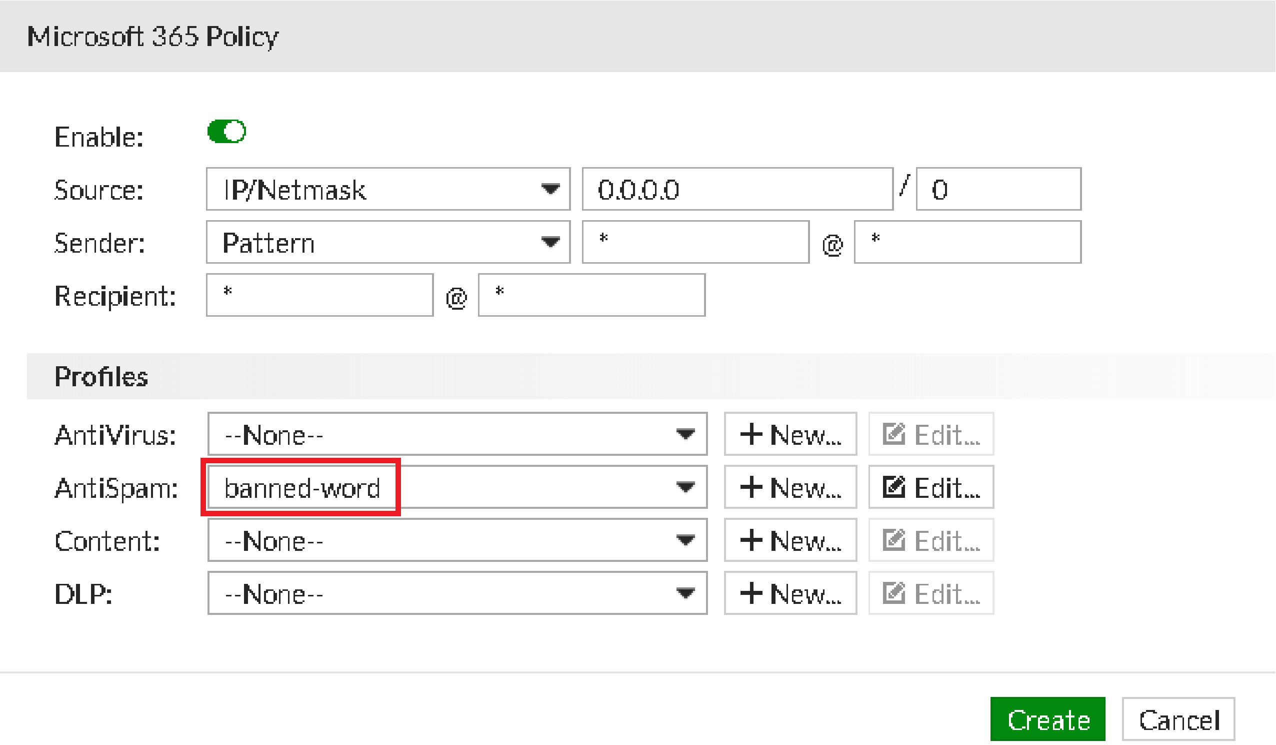
6. Click *OK*, then click *Create*.

To configure the real-time scan policy:

1. Go to *Policy* > *Real-time Scan* > *Policy* and click *New*.
2. Enable the policy, and define the *Source*, *Sender*, and *Recipient* information.

> For testing purposes, this policy is left to accept all sources and to all recipients registered to the Microsoft 365 account.
>
> In cases that the FortiMail unit has multiple Microsoft 365 accounts registered, you could set the *Recipient* email domain (*@<domain>) to a specific domain, applying this real-time scan policy to only a specific Microsoft 365 account.

3. Under *Profiles*, set *AntiSpam* to the *banned-word* profile you created earlier.
   Any email meeting the banned word search criteria will be discarded, as specified in the profile.
4. Click *Create*.



Microsoft 365 Policy

Enable: ●

Source: IP/Netmask 0.0.0.0 / 0

Sender: Pattern * @ *

Recipient: * @ *

Profiles

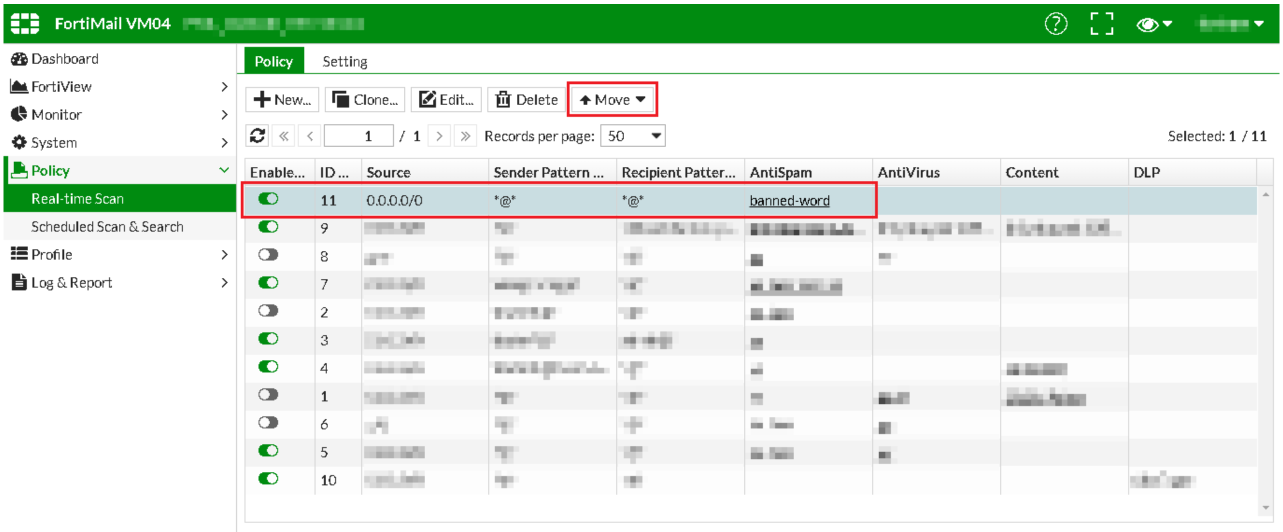
AntiVirus: --None--

AntiSpam: banned-word

Content: --None--

DLP: --None--

5. When created, select the policy from the policy table and click *Move* and move it *Up* to the top of the list.

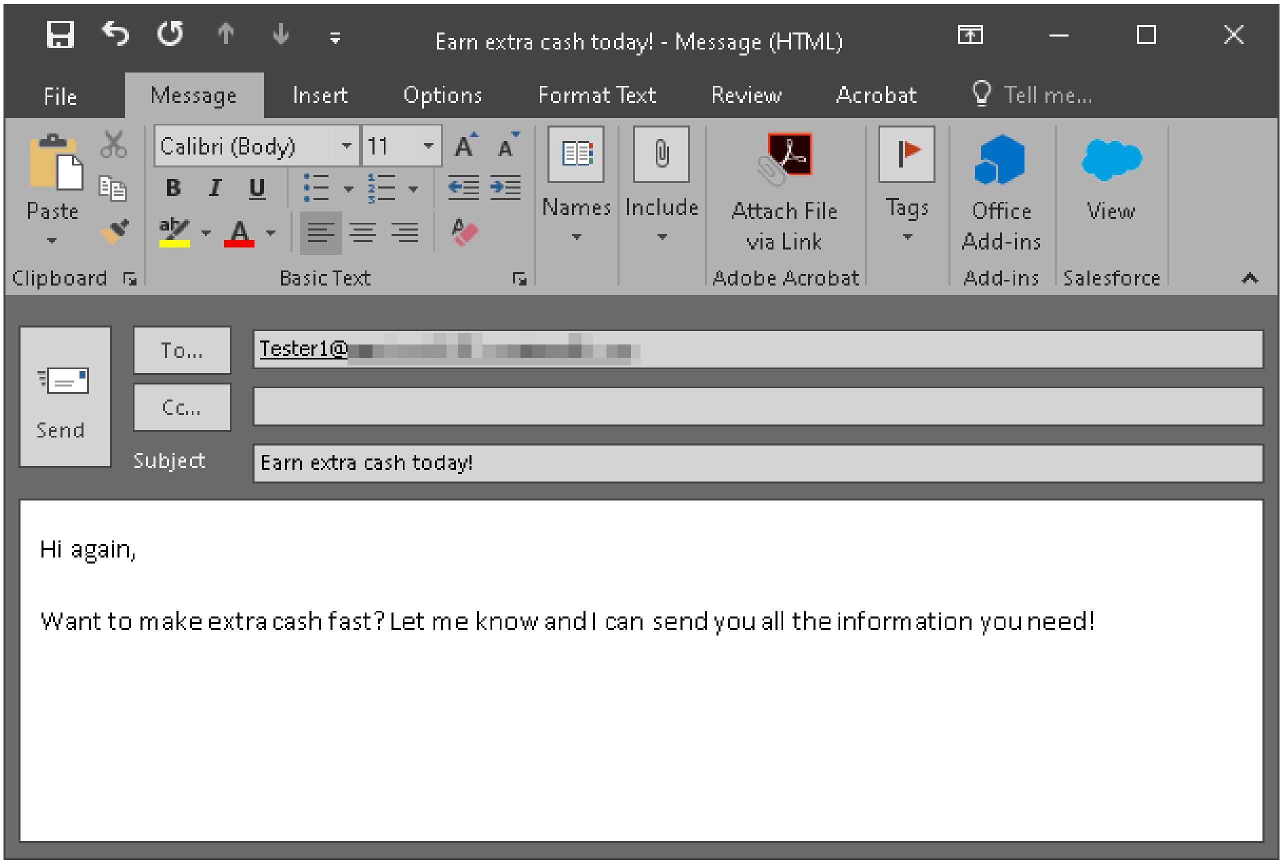


Records per page: 50 | Page 1 / 1 | Selected: 1 / 11

Enable...	ID ...	Source	Sender Pattern ...	Recipient Patter...	AntiSpam	AntiVirus	Content	DLP
●	11	0.0.0.0/0	*@*	*@*	banned-word			
●	9	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	
○	8	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]		
●	7	[redacted]	[redacted]	[redacted]	[redacted]			
○	2	[redacted]	[redacted]	[redacted]	[redacted]			
●	3	[redacted]	[redacted]	[redacted]	[redacted]			
●	4	[redacted]	[redacted]	[redacted]	[redacted]		[redacted]	
○	1	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	
○	6	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]		
●	5	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]		
●	10	[redacted]	[redacted]	[redacted]				[redacted]

Results

1. Send an email to a user's email address that is registered to the Microsoft 365 account.
   In this example, the email's *Subject* contains the banned word string to simulate a spam email.



To: Tester1@[redacted]

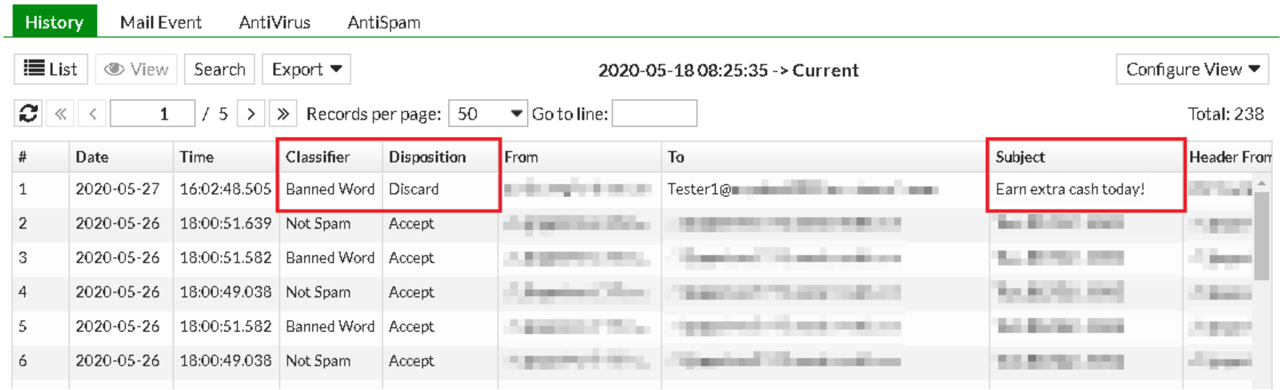
Subject: Earn extra cash today!

Hi again,

Want to make extra cash fast? Let me know and I can send you all the information you need!

2. In FortiMail, from the *Microsoft 365 View*, go to *Monitor* > *Log* > *History*.

The email appears in the log entries, showing the triggering *Classifier* and the *Disposition* as the resulting action.



2020-05-18 08:25:35 -> Current

1 / 5 Records per page: 50

Total: 238

#	Date	Time	Classifier	Disposition	From	To	Subject	Header From
1	2020-05-27	16:02:48.505	Banned Word	Discard	[redacted]	Tester1@[redacted]	Earn extra cash today!	[redacted]
2	2020-05-26	18:00:51.639	Not Spam	Accept	[redacted]	[redacted]	[redacted]	[redacted]
3	2020-05-26	18:00:51.582	Banned Word	Accept	[redacted]	[redacted]	[redacted]	[redacted]
4	2020-05-26	18:00:49.038	Not Spam	Accept	[redacted]	[redacted]	[redacted]	[redacted]
5	2020-05-26	18:00:51.582	Banned Word	Accept	[redacted]	[redacted]	[redacted]	[redacted]
6	2020-05-26	18:00:49.038	Not Spam	Accept	[redacted]	[redacted]	[redacted]	[redacted]

(Optional) Hiding email on arrival

With the introduction of real-time scanning to FortiMail 6.4.0, there is still the inherent risk that user's may open potentially dangerous emails in Microsoft 365 before the FortiMail unit has had the opportunity to scan the email, especially if the email contains large attachments.

To mitigate this risk, enable `hide-email-on-arrival` to automatically move email to a hidden folder on arrival for it to be subjected to real-time scanning. Only after the email is scanned and deemed safe is it then removed from the hidden folder and placed into the user's mailbox.

This feature (disabled by default) can only be enabled using the *CLI Console*.

To enable this feature, open the *CLI Console* and enter the following:

```
config ms365 setting
   edit <name>
      set hide-email-on-arrival enable
end
```

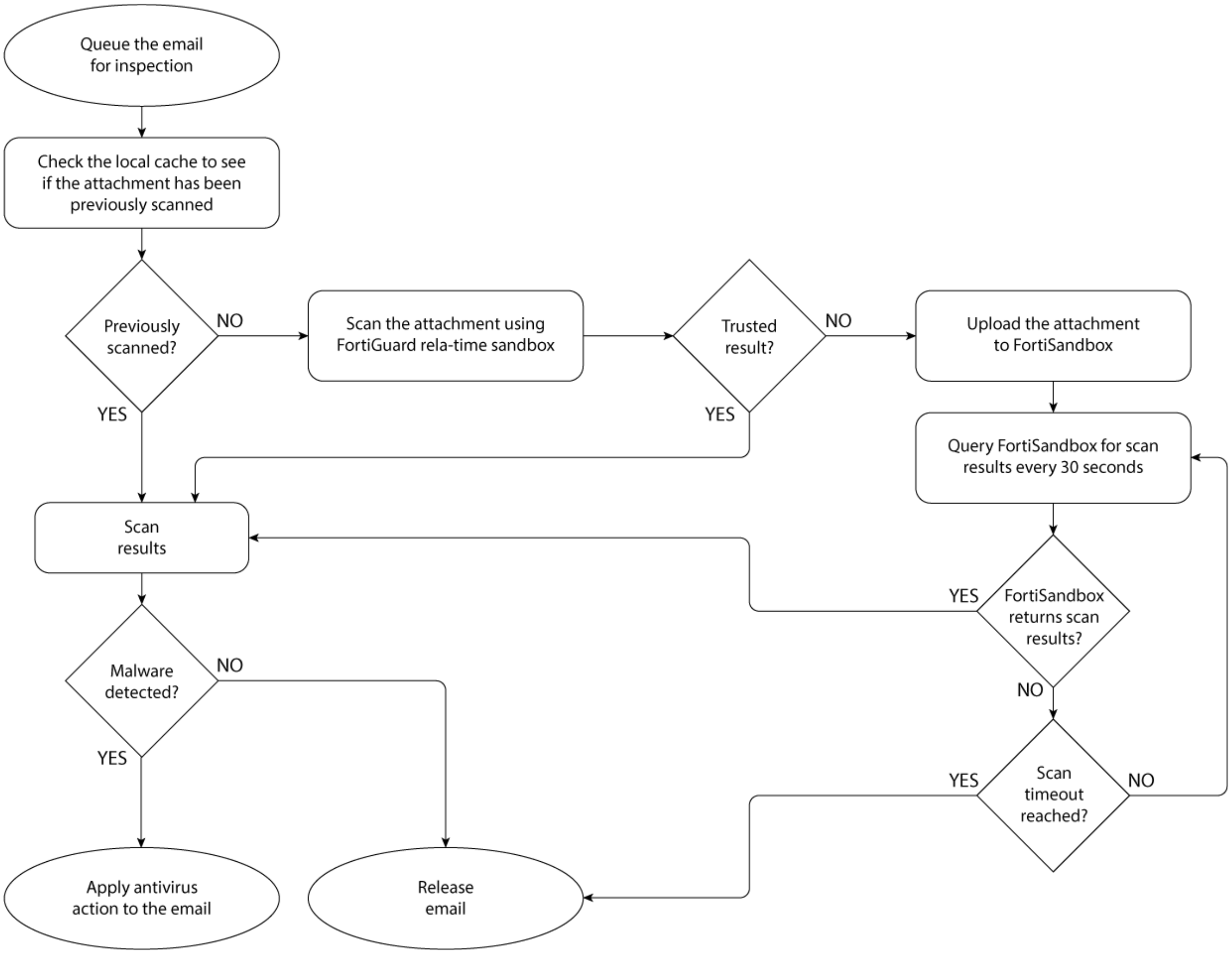
Integrating FortiSandbox with FortiMail

FortiSandbox is a key Fortinet product in providing an innovative Advanced Threat Protection (ATP) solution. Recommended by NSS Labs, FortiSandbox is designed to detect and analyze advanced targeted attacks designed to bypass traditional security defenses.

While traditional signature-based systems rely on predefined virus signatures to catch viruses, FortiSandbox looks at the construction of files for characteristics commonly found in viruses and emulates the execution looking for typical virus behavior. As a file is examined, the virus-like attributes are totaled. If a threshold in the number of virus-like attributes is passed, the file is marked as suspicious.

This recipe shows how to integrate FortiSandbox with FortiMail. As part of this integration, an AntiVirus profile on the FortiMail is created, allowing the FortiMail unit to send potentially harmful attachments to the FortiSandbox unit for further analysis.

The workflow below shows the scanning process.


Queue the email for inspection
Check the local cache to see if the attachment has been previously scanned
Previously scanned?
NO
YES
Scan the attachment using FortiGuard rela-time sandbox
Trusted result?
NO
YES
Upload the attachment to FortiSandbox
Query FortiSandbox for scan results every 30 seconds
Scan results
YES
FortiSandbox returns scan results?
NO
Malware detected?
NO
YES
YES
Scan timeout reached?
NO
Apply antivirus action to the email
Release email

Note that the supported file types and extensions that the FortiMail unit can submit to the FortiSandbox unit is dynamic, and can change depending on the version of the two products. Below is a list of all supported file types and extensions as of FortiMail 5.2.3 and FortiSandbox 2.0 and later:

- MS Word: docx, dotx, docm, dotm
- MS Excel: xlsx, xlsm, xltm, xlsb, xlam
- MS PowerPoint: pptx, ppsx, potx, sldx, pptm, ppsm, potm, ppam, sldm
- MS OneNote: onetoc
- MS Theme: thmx
- JAR
- SWF
- PDF
- Java script file
- Windows executable files such as .scr, .dll, .com, and .exe
- Archive files: .RAR and .ZIP

Connecting FortiSandbox to FortiMail

You may connect a physical FortiSandbox unit to the FortiMail unit, or you can purchase the FortiSandbox cloud service, allowing the use of the FortiSandbox antivirus service without owning your own FortiSandbox appliance.

Depending on your FortiCare contract, FortiSandbox cloud provides two types of services:

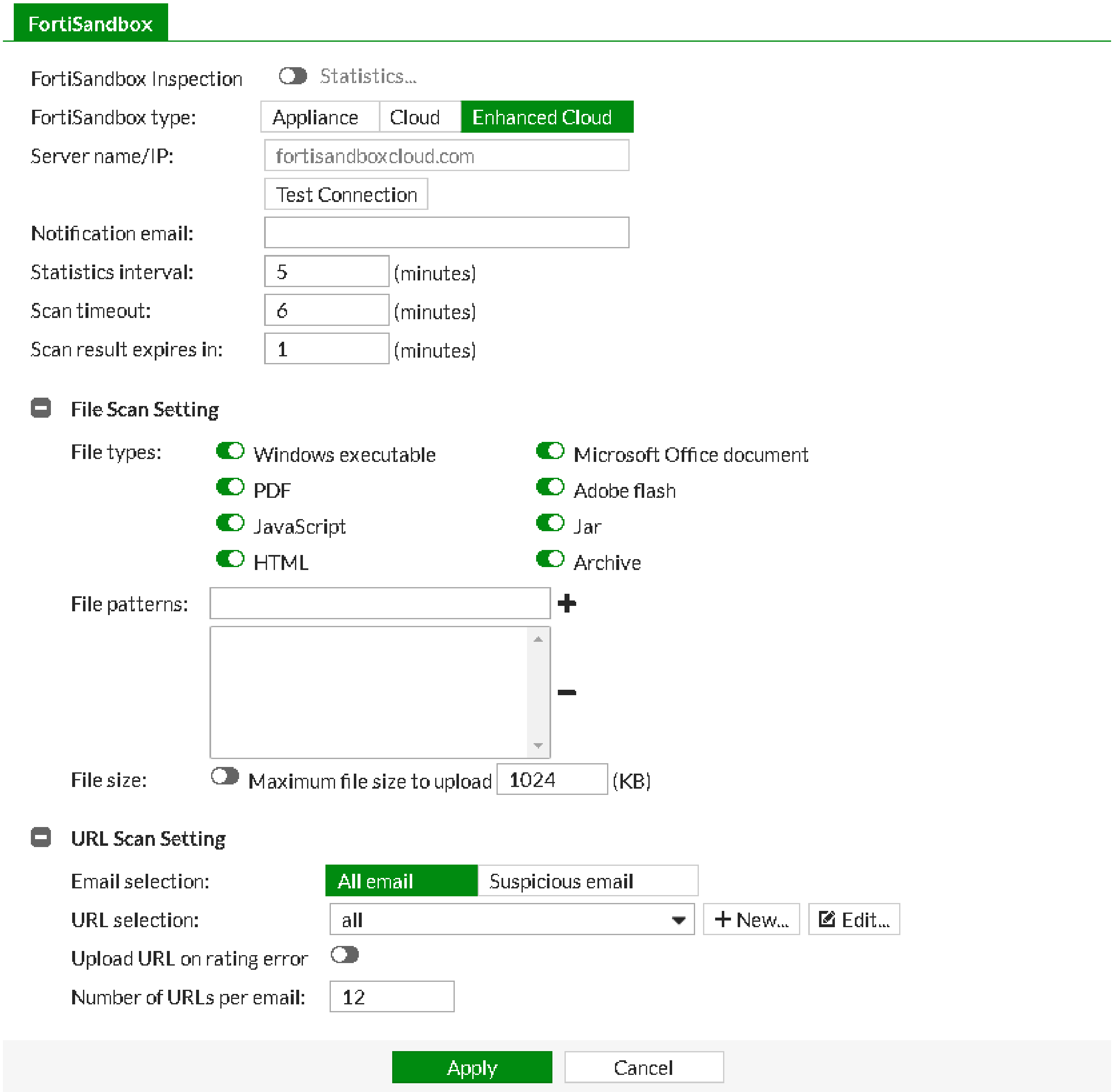
- Regular cloud service: You can use one FortiCare account to register multiple FortiMail units.
- Enhanced cloud service: You can only register one FortiMail unit with one FortiCare account to guarantee dedicated FortiSandbox service and high performance.

Both FortiSandbox regular and enhanced cloud services require a valid FortiCloud license. For more information, see FortiCloud service in the FortiMail Administration Guide.

1. On FortiMail, go to **System > FortiSandbox > FortiSandbox** and enable **FortiSandbox Inspection**.
2. Set **FortiSandbox type** to either **Appliance**, **Cloud**, or **Enhanced Cloud**.
   If you are connecting to a physical FortiSandbox, or you have an enhanced cloud service subscription, set **Server name/IP** to the IP address or FQDN (respectively) of the FortiSandbox unit.
3. Set **Notification email** to the administrator's email address to be notified of protection activity.
4. Set **Statistics interval** to the duration of time in minutes the FortiMail unit should wait before retrieving high level statistics from the FortiSandbox unit.
5. Under **File Scan Settings**, enable the various **File types** you want to submit to the FortiSandbox unit.
6. Optionally, define any **File patterns** you would like to submit (for example, `*.txt` for any text-files), and specify the **Maximum file size to upload** to FortiSandbox, which may improve performance.
7. Under **URI Scan Settings**, define whether **All email** or **Suspicious email** should be submitted to the FortiSandbox unit.
8. Set **URI selection** to a system-defined URI filter profile from the drop-down menu, or create and assign your own. URI filter profiles use various FortiGuard categories as a filter for catching suspicious email content.
9. Enable **Upload URI on rating error** to upload URIs to FortiSandbox for scanning, in cases where the FortiMail unit may not be able to retrieve FortiGuard query results due to network connection failure. Enabling this option may affect the FortiSandbox unit's performance.

10. Set Number of URIs per email to the total number of URIs that will be scanned per email.
11. Click **Apply**.

A statistics report can be viewed anytime by clicking **Statistics**, showing the various file types submitted, and whether they are considered clean or malicious, and high, medium, or low risk. Statistics can be viewed for **This Hour**, **Today**, or **This Week**.



FortiSandbox Inspection: off

FortiSandbox type: Appliance | Cloud | **Enhanced Cloud**

Server name/IP: fortisandboxcloud.com

Notification email:

Statistics interval: 5 (minutes)

Scan timeout: 6 (minutes)

Scan result expires in: 1 (minutes)

File Scan Setting

File types: Windows executable (on), Microsoft Office document (on), PDF (on), Adobe flash (on), JavaScript (on), Jar (on), HTML (on), Archive (on)

File patterns:

File size: off Maximum file size to upload 1024 (KB)

URL Scan Setting

Email selection: **All email** | Suspicious email

URL selection: all

Upload URL on rating error: off

Number of URLs per email: 12

Creating an AntiVirus profile

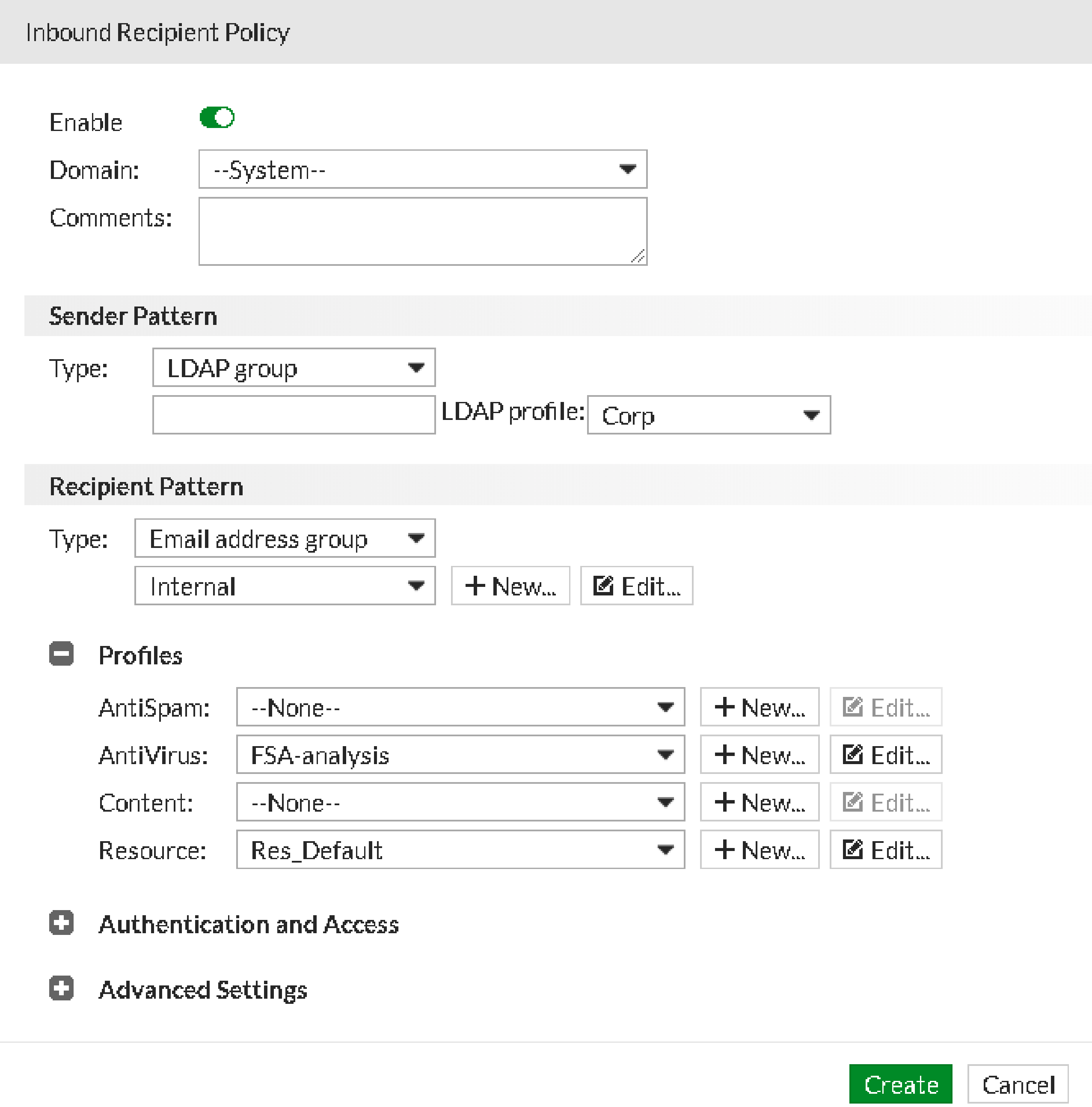
1. Go to **Profile > AntiVirus > AntiVirus** and click **New**.
2. Assign a specific **Domain** if necessary, otherwise leave it as a **System** based profile.
3. Enter a **Profile name**.
4. Set **Default action** to an antivirus action profile. For this example, set to **SystemQuarantine**.
   Note that, in this case, if you set **Default action** to **Reject**, the actual action taken will be to fallback to system quarantine, since email messages are to be sent to the FortiSandbox unit.
5. Under **FortiSandbox**, set the default **Scan mode**: **Submit and wait for result** to wait for scan results before delivering the email, or **Submit only** to submit emails to FortiSandbox and still deliver the email without waiting for the scan results.
6. Enable **Attachment analysis** to send email attachments to the FortiSandbox unit.
7. Enable **URI analysis** to send the URIs to the FortiSandbox unit.
8. Under **Attachment analysis** and **URI analysis** specify the action to take if the FortiSandbox analysis determines that an email has a virus or other threat attributes. You can specify different actions according to threat level. Each threat level action is set by default to use the **Default action** of the antivirus profile.
9. Click **Create**.

Creating a security policy

You must apply the newly created antivirus profile to a security policy for inbound traffic.

1. Go to **Policy > Recipient Policy > Inbound** and click **New**.
   Note that a security policy applying the antivirus profile can also be created under **Policy > IP Policy > IP Policy**.
2. Click **Enable**.
3. Define which groups this inbound recipient-based policy applies to under **Sender Pattern** and **Recipient Pattern**. In the example below, this policy applies to the **Corp** LDAP group sending any email to the **Internal** email address group.
4. Under **Profiles**, set **AntiVirus** to the newly created antivirus profile.

5. Click **Create**.



Inbound Recipient Policy

Enable

Domain: --System--

Comments:

Sender Pattern

Type: LDAP group

LDAP profile: Corp

Recipient Pattern

Type: Email address group

Internal

Profiles

AntiSpam: --None--

AntiVirus: FSA-analysis

Content: --None--

Resource: Res_Default

Authentication and Access

Advanced Settings

Remote logging in FortiMail using FortiAnalyzer

You can remotely store log messages on your FortiAnalyzer, in order to avoid storing your FortiMail log information to your local hard disk.

Configuring remote logging

1. Go to **Log & Report > Log Setting > Remote** and click **New**.
2. Click **Enable** and enter a **Profile name**.
3. Set **Address** to the IP address of the FortiAnalyzer.
4. Set **Port** to **514**, the commonly used port for syslog events that FortiAnalyzer uses to listen for incoming syslog event notifications.
5. Select a security **Level** that a log message must meet or exceed in order to be recorded and stored.
6. Select the **Facility** identifier that the FortiMail unit uses to identify itself.
7. Set the **Log protocol** to **Syslog** or **OFTPS** (FortiAnalyzer units support both protocols).
8. In this example, disable **CSV format**, as FortiAnalyzer units do not support CSV-formatted log messages.
9. Enable **Matched session only** if you want to send only the matched session logs to the remote server, otherwise all logs will be sent regardless.
10. Under **Logging Policy Configuration**, enable the types of logs you want to record to the FortiAnalyzer unit.
11. Click **Create**.

Using SMTP authentication in FortiMail

SMTP authentication can help mitigate brute force password attacks by tracking the IP addresses of the offending client attempting to connect to the box. SMTP authentication can detect, block, and punish hackers.

This recipe guides you through the process of enabling SMTP authentication and checking the SMTP authentication score and record. This recipe is undertaken solely in the CLI.

Enabling SMTP authentication

Go to **Dashboard > Console**, click inside the console, and enter the following command. Also, if there is a gateway before the mail server, add the gateway to the exempt list, as shown below:

```
config system security authserver
   set status enable
   config exempt-list
      edit 1
         set sender-ip-mask 172.20.140.232/32
      next
   end
end
```

Checking SMTP authorization score and record

1. To display automatically added IP addresses, enter the following CLI command:
   `diagnose system authserver auto-exempt display`
   To delete the IP address, enter the following:
   `diagnose system authserver auto-exempt delete xxxx`
2. To display the `iptables` statistics for currently blocked IP addresses, enter the following command:
   `diagnose system authserver iptables ipv4`
3. To view the authentication records for a specific IP address, enter the following command:
   `diagnose system authserver records 172.20.140.230`
4. To view the authentication status of a specific IP address, showing whether it is safe or blocked, enter the following command:
   `diagnose system authserver status 172.20.140.231`

Upgrading FortiMail firmware in HA mode

This recipe shows how to perform seamless firmware upgrade for all units in an HA cluster, in either active-passive or config-only.

Similar to upgrading the firmware of a standalone FortiMail unit, config-only HA clusters will have normal email processing temporarily interrupted while firmware is being installed on the primary unit. However, if the HA group is active-passive, when the primary unit has its firmware upgraded, the primary unit sends a holdoff command to the secondary unit. This avoids any undue email traffic interruptions, and prevents the secondary unit from taking over the primary-role during the primary unit's reboot (unless otherwise specified).

Regardless of whether the HA cluster is in active-passive or config-only mode, the secondary unit/s must always upgrade their firmware before the primary unit.

Upgrade firmware on each FortiMail unit according to the upgrade path specified in the release notes.

For the purpose of this recipe, you should be aware of the following:

- The primary unit has an IP address of 172.20.142.198
- The secondary unit has an IP address of 172.20.142.228
- The units are being upgraded from version 6.4.0 to 6.4.1

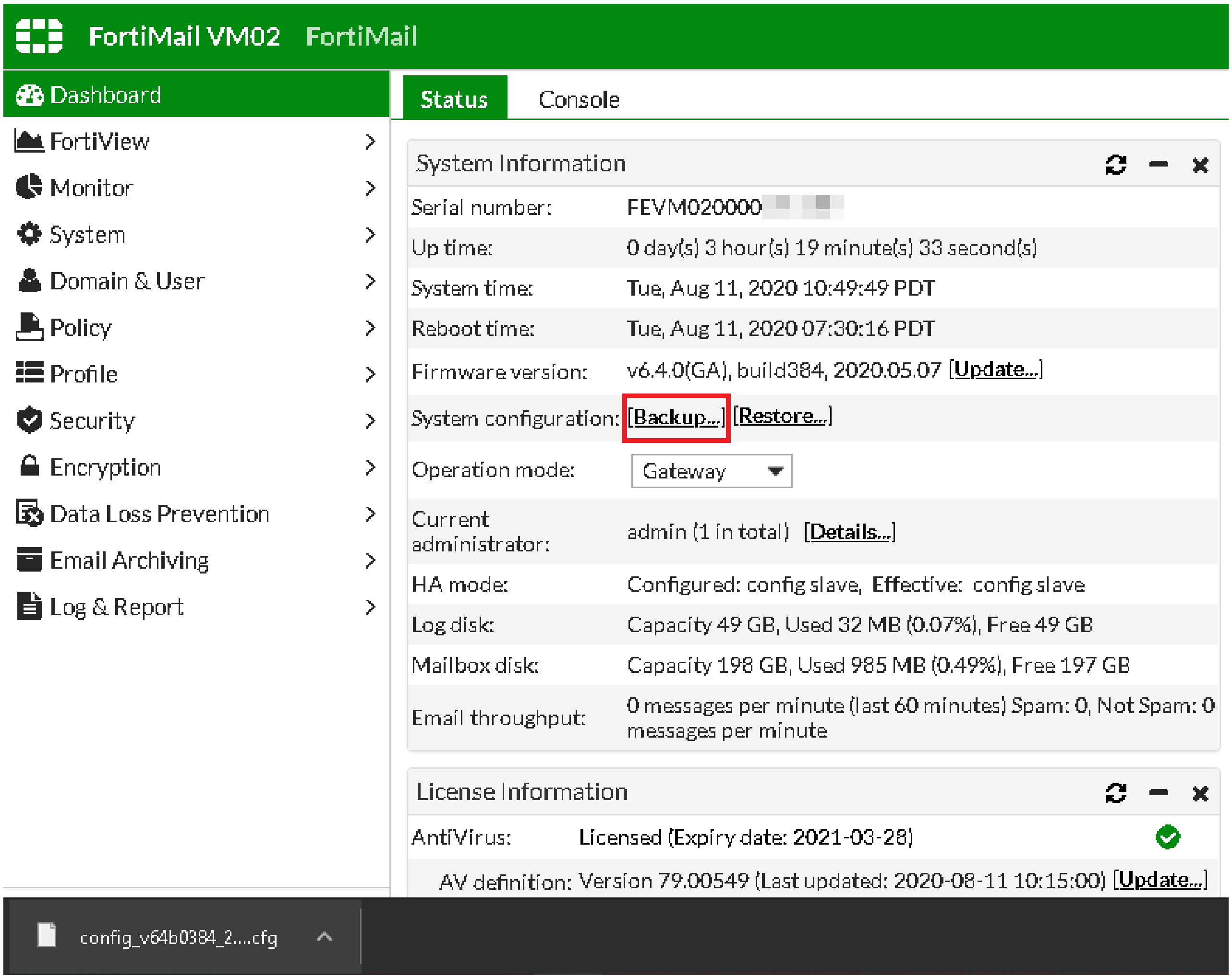
For more detailed information on FortiMail units operating as an HA group, see the Using high availability (HA) section of the FortiMail Administration Guide.

Firmware configuration backup

Before undertaking a firmware upgrade, it is strongly recommended to back up the configuration on both the primary and the secondary units:

1. On each unit, go to *Dashboard* > *Status*.
2. In the *System Information* widget, under *System configuration*, click *Backup*.
   Optionally, add *Encryption* to your backup config file.
3. Click *OK*.

A config file is downloaded to your local computer.



Serial number:	FEVM020000[redacted]
Up time:	0 day(s) 3 hour(s) 19 minute(s) 33 second(s)
System time:	Tue, Aug 11, 2020 10:49:49 PDT
Reboot time:	Tue, Aug 11, 2020 07:30:16 PDT
Firmware version:	v6.4.0(GA), build384, 2020.05.07 [Update...]
System configuration:	[Backup...] [Restore...]
Operation mode:	Gateway
Current administrator:	admin (1 in total) [Details...]
HA mode:	Configured: config slave, Effective: config slave
Log disk:	Capacity 49 GB, Used 32 MB (0.07%), Free 49 GB
Mailbox disk:	Capacity 198 GB, Used 985 MB (0.49%), Free 197 GB
Email throughput:	0 messages per minute (last 60 minutes) Spam: 0, Not Spam: 0 messages per minute

AntiVirus: Licensed (Expiry date: 2021-03-28) ✓

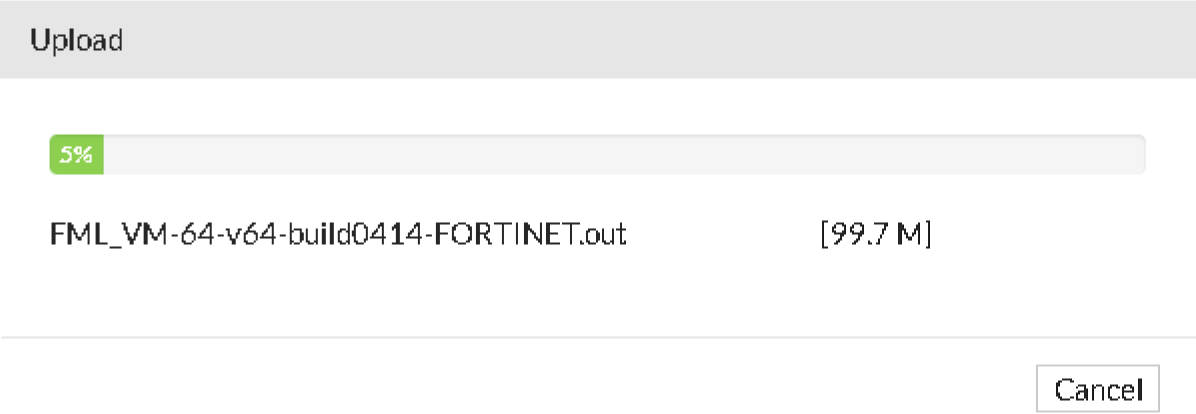
AV definition: Version 79.00549 (Last updated: 2020-08-11 10:15:00) [Update...]

HA group firmware upgrade

Once the configuration files for each HA cluster member have been backed up, the firmware upgrade can begin.

⚠ When installing or upgrading firmware to an HA group, you must install firmware on the secondary unit/units before installing firmware on the primary unit.

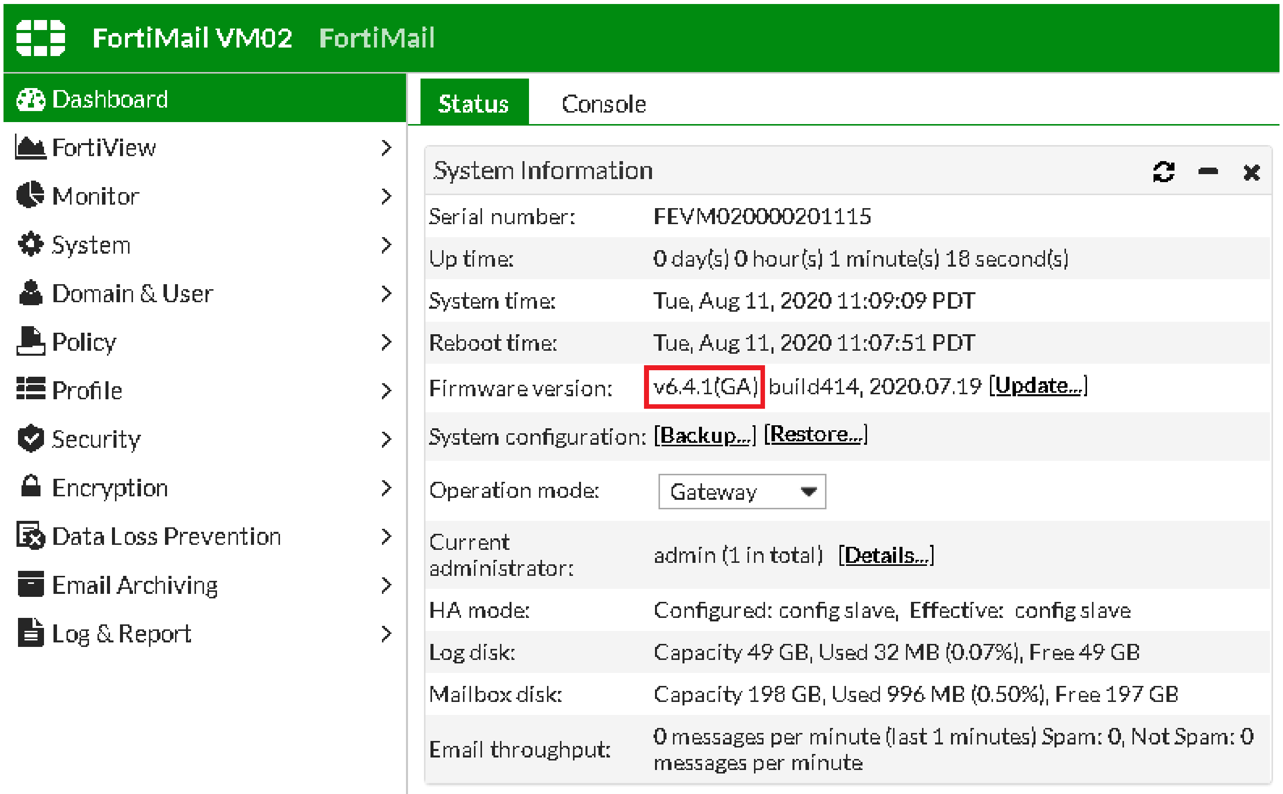
1. On the secondary unit, go to *Dashboard* > *Status*.
2. In the *System Information* widget, under *Firmware version*, click *Update*.
   A prompt appears showing that the firmware file is being uploaded.



FML_VM-64-v64-build0414-FORTINET.out [99.7 M]

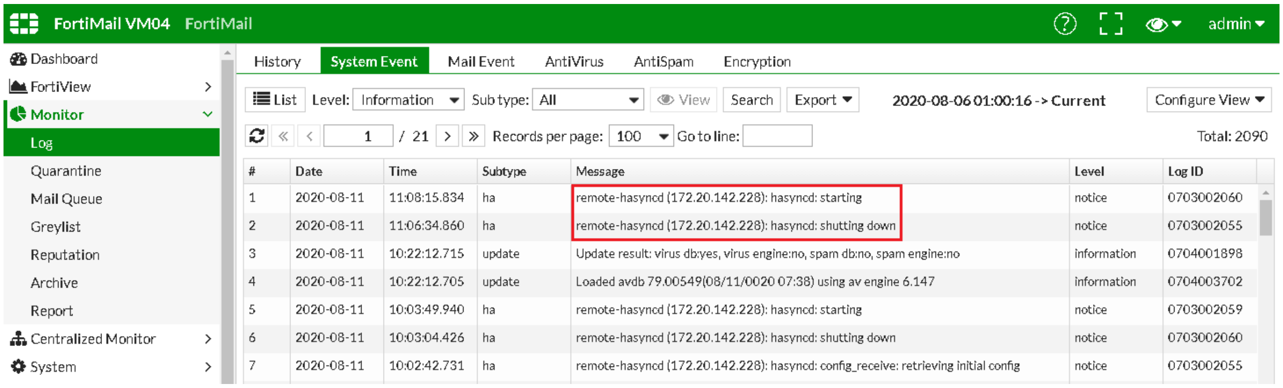
Once uploaded, a prompt appears asking if you are sure you want to update.

3. Click *OK*. The unit then reboots.
   After the reboot has completed, you may need to refresh the page.
   You are then redirected to the login page.
4. Login to the FortiMail unit, and confirm that the secondary unit has successfully updated its firmware.



Serial number:	FEVM020000201115
Up time:	0 day(s) 0 hour(s) 1 minute(s) 18 second(s)
System time:	Tue, Aug 11, 2020 11:09:09 PDT
Reboot time:	Tue, Aug 11, 2020 11:07:51 PDT
Firmware version:	v6.4.1(GA) build414, 2020.07.19 [Update...]
System configuration:	[Backup...] [Restore...]
Operation mode:	Gateway
Current administrator:	admin (1 in total) [Details...]
HA mode:	Configured: config slave, Effective: config slave
Log disk:	Capacity 49 GB, Used 32 MB (0.07%), Free 49 GB
Mailbox disk:	Capacity 198 GB, Used 996 MB (0.50%), Free 197 GB
Email throughput:	0 messages per minute (last 1 minutes) Spam: 0, Not Spam: 0 messages per minute

5. On the primary unit, go to *Monitor* > *Log* > *System Event* and confirm the reboot event of the secondary unit (172.20.142.228).



2020-08-06 01:00:16 -> Current

Total: 2090

#	Date	Time	Subtype	Message	Level	Log ID
1	2020-08-11	11:08:15.834	ha	remote-hasyncd (172.20.142.228): hasyncd: starting	notice	0703002060
2	2020-08-11	11:06:34.860	ha	remote-hasyncd (172.20.142.228): hasyncd: shutting down	notice	0703002055
3	2020-08-11	10:22:12.715	update	Update result: virus db:yes, virus engine:no, spam db:no, spam engine:no	information	0704001898
4	2020-08-11	10:22:12.705	update	Loaded avdb 79.00549(08/11/0020 07:38) using av engine 6.147	information	0704003702
5	2020-08-11	10:03:49.940	ha	remote-hasyncd (172.20.142.228): hasyncd: starting	notice	0703002059
6	2020-08-11	10:03:04.426	ha	remote-hasyncd (172.20.142.228): hasyncd: shutting down	notice	0703002060
7	2020-08-11	10:02:42.731	ha	remote-hasyncd (172.20.142.228): hasyncd: config_receive: retrieving initial config	notice	0703002055

6. On the primary unit, upgrade the firmware the same way as the secondary unit.
   All units have been upgraded to the same firmware version.

HA cluster central monitoring

With a valid MSSP license from FortiGuard, you may verify the HA cluster status and log activity under *Centralized Monitor* > *Overview* > *Overview Status*.

For more information about the centralize monitoring feature, see the Centrally monitoring the HA cluster section of the FortiMail Administration Guide.