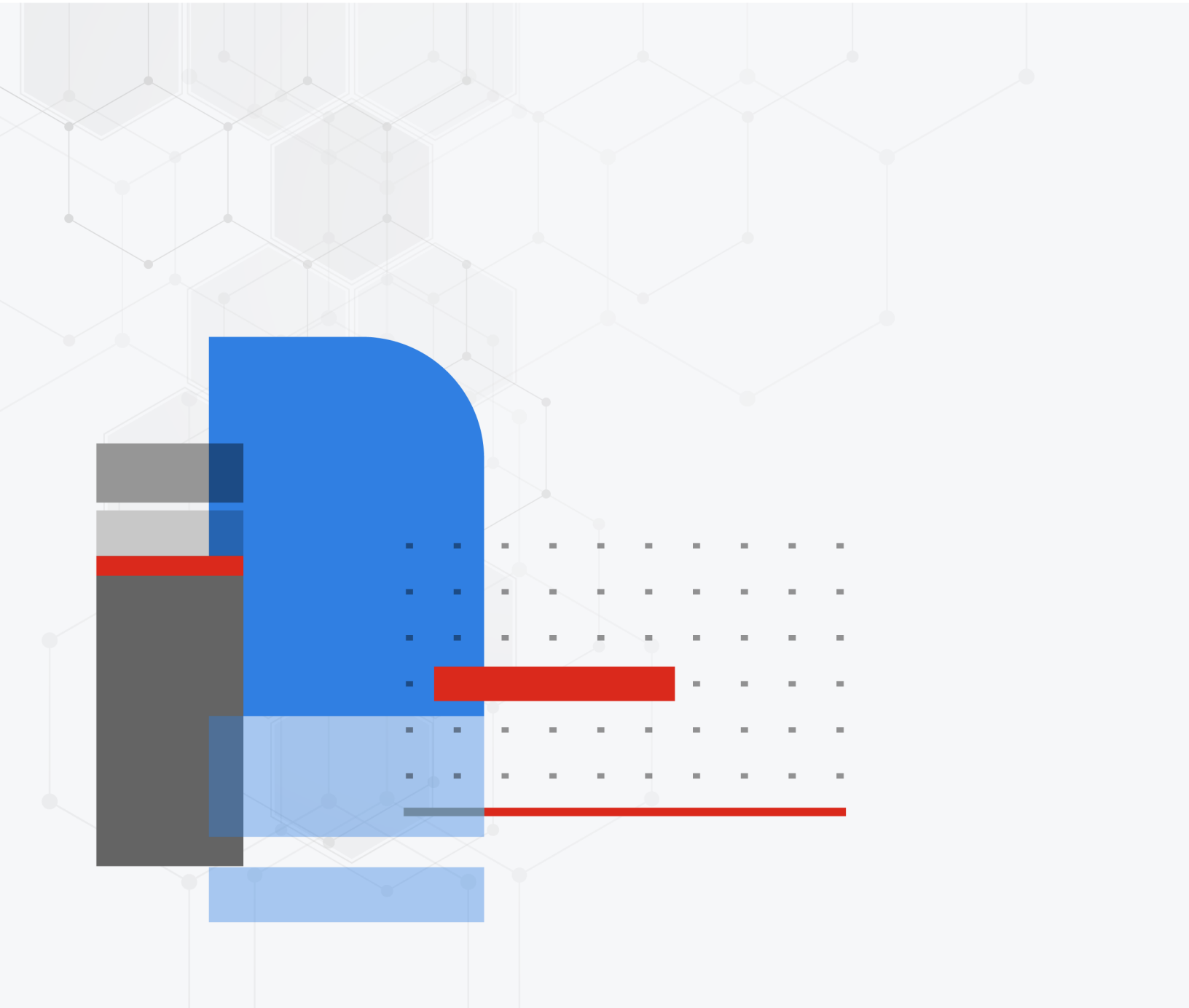




# Cookbook

FortiMail 7.4.2



**FORTINET DOCUMENT LIBRARY**

<https://docs.fortinet.com>

**FORTINET VIDEO LIBRARY**

<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/training-certification>

**FORTINET TRAINING INSTITUTE**

<https://training.fortinet.com>

**FORTIGUARD LABS**

<https://www.fortiguard.com>

**END USER LICENSE AGREEMENT**

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

**FEEDBACK**

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

February 27, 2024

FortiMail 7.4.2 Cookbook

06-742-000000-20240214

# TABLE OF CONTENTS

|                                                                 |           |
|-----------------------------------------------------------------|-----------|
| <b>Change Log</b>                                               | <b>6</b>  |
| <b>Authentication</b>                                           | <b>7</b>  |
| Microsoft AD Domain Service for FortiMail LDAP profile          | 7         |
| Creating the Azure AD Domain Services instance                  | 7         |
| Enabling Secure LDAP for external access                        | 8         |
| Adding the Azure AD member to AAD DC Administrator group        | 9         |
| Configuring the FortiMail for recipient address verification    | 11        |
| Microsoft Entra ID as SAML IdP for FortiMail SSO authentication | 12        |
| Configuring Azure AD for SSO with an application                | 13        |
| Configuring SSO on FortiMail                                    | 14        |
| <b>AntiSpam</b>                                                 | <b>16</b> |
| Configuring adult image analysis in FortiMail                   | 17        |
| Configuring a Content Profile and Scan Options                  | 17        |
| Establishing adult image analysis                               | 19        |
| Configuring banned words in FortiMail                           | 20        |
| Configuring banned word options in an AntiSpam Profile          | 20        |
| Configuring safelist word options                               | 22        |
| Mitigating spam attacks with weighted analysis profiles         | 23        |
| Creating a dictionary and weighted analysis profile             | 24        |
| Assigning the weighted analysis profile to the antispam profile | 28        |
| Configuring the inbound policy for weighted analysis            | 29        |
| Blocking the email of a known threat                            | 31        |
| Configuring access controls                                     | 31        |
| Configuring policies                                            | 32        |
| Downloading oversized email attachments                         | 34        |
| Configuring MS Exchange                                         | 34        |
| Configuring notification profiles                               | 35        |
| Configuring content profiles and recipient profiles             | 38        |
| Increasing size limits in session profiles                      | 40        |
| Configuring incoming email DMARC checking with SPF and DKIM     | 41        |
| Enabling SPF checking for incoming email                        | 41        |
| Enabling DKIM checking for incoming email                       | 43        |
| Enabling DMARC checking for incoming email                      | 45        |
| FortiGuard AntiSpam service with FortiMail                      | 47        |
| Connecting to FortiGuard AntiSpam service                       | 47        |
| Creating an AntiSpam profile                                    | 48        |
| Using the AntiSpam profile in a policy                          | 48        |
| FortiGuard AntiVirus service with FortiMail                     | 50        |
| Connecting to FortiGuard AntiVirus service                      | 50        |
| Creating an AntiVirus profile                                   | 51        |
| Using the AntiVirus profile in a policy                         | 52        |
| Preventing an ISP from being blocklisted                        | 53        |
| Enabling transparent mode                                       | 53        |
| Configuring the connection with the RADIUS server               | 53        |

|                                                             |           |
|-------------------------------------------------------------|-----------|
| Testing the FortiMail .....                                 | 54        |
| Removing the network interfaces from the bridge .....       | 54        |
| Configuring the session profiles .....                      | 55        |
| Configuring IP-based policies .....                         | 57        |
| Configuring the outgoing proxy .....                        | 59        |
| Configuring policy-based routes on the router .....         | 59        |
| Protecting against email impersonation in FortiMail .....   | 60        |
| Creating an impersonation analysis profile .....            | 60        |
| Activating the impersonation profile .....                  | 61        |
| Viewing the impersonation analysis logs .....               | 61        |
| Configuring dynamic scanning .....                          | 61        |
| Preparing DMARC checking for outbound email .....           | 63        |
| Enabling DKIM signing on FortiMail .....                    | 64        |
| Retrieving public DNS record information .....              | 65        |
| Testing email signing and verification .....                | 67        |
| <b>Best practices .....</b>                                 | <b>70</b> |
| Resetting a lost administrator password .....               | 71        |
| Physically connect the FortiMail unit .....                 | 71        |
| Connect to the FortiMail unit using terminal software ..... | 72        |
| Log in using the maintainer account .....                   | 73        |
| Change the admin password .....                             | 73        |
| <b>Getting started .....</b>                                | <b>74</b> |
| How to set up an active-passive HA in FortiMail .....       | 75        |
| Configuring HA .....                                        | 75        |
| Configuring interface monitoring .....                      | 76        |
| Configuring alert emails in FortiMail .....                 | 77        |
| Configuring alert recipients .....                          | 77        |
| Configuring alert categories .....                          | 77        |
| Backing up and restoring mail data in FortiMail .....       | 78        |
| Configuring mailbox backup .....                            | 78        |
| Restoring from a backup .....                               | 79        |
| How to set up a config-only HA in FortiMail .....           | 80        |
| Configuring mail data storage on a NAS server .....         | 80        |
| Configuring HA .....                                        | 81        |
| Custom replacement messages in FortiMail .....              | 83        |
| Configuring a custom message .....                          | 83        |
| Deploying FortiMail Gateway mode .....                      | 84        |
| Connecting to FortiMail .....                               | 84        |
| Setting up FortiMail .....                                  | 84        |
| Configuring DNS records .....                               | 85        |
| Configuring firewall policies .....                         | 85        |
| Configuring MUAs to use FortiMail .....                     | 85        |
| Testing the installation .....                              | 85        |
| Deploying FortiMail Server mode .....                       | 87        |
| Accessing Server mode .....                                 | 87        |
| Configuring DNS records .....                               | 87        |
| Configuring firewall policies .....                         | 88        |

|                                                                        |     |
|------------------------------------------------------------------------|-----|
| Adding email user accounts .....                                       | 88  |
| Configuring MUAs to use for FortiMail .....                            | 88  |
| Testing the installation .....                                         | 89  |
| Deploying FortiMail Transparent mode .....                             | 90  |
| Connecting to FortiMail from your PC .....                             | 90  |
| Running the Quick Start Wizard .....                                   | 90  |
| Configuring DNS records .....                                          | 90  |
| Configuring proxies .....                                              | 91  |
| Testing the installation .....                                         | 91  |
| Encrypting confidential emails in FortiMail .....                      | 92  |
| Enabling the IBE service .....                                         | 92  |
| Configuring the encryption profile .....                               | 93  |
| Configuring the content action profile .....                           | 94  |
| Creating the dictionary profile .....                                  | 94  |
| Configuring the content profile .....                                  | 95  |
| Configuring policies .....                                             | 95  |
| How to encrypt emails sent from a designated source in FortiMail ..... | 96  |
| Enabling the IBE services .....                                        | 96  |
| Configuring the encryption profile .....                               | 97  |
| Configuring delivery rules .....                                       | 98  |
| How to integrate FortiMail into Microsoft 365 .....                    | 99  |
| Configuring domain and DNS settings in Office 365 .....                | 99  |
| Configuring FortiMail to accept Office 365 .....                       | 100 |
| Configuring Office 365 to accept FortiMail .....                       | 101 |
| Configuring outbound settings in FortiMail .....                       | 106 |
| Configuring outbound settings in Office 365 .....                      | 106 |
| Installing FortiMail firmware using the CLI .....                      | 109 |
| Connecting the hardware .....                                          | 109 |
| Installing the firmware .....                                          | 109 |
| Reconnecting to the FortiMail unit after a downgrade .....             | 110 |
| Restoring the configuration .....                                      | 110 |
| Configuring and viewing FortiMail log messages .....                   | 111 |
| Enabling and configuring log settings .....                            | 111 |
| Monitoring and downloading log messages .....                          | 111 |
| Integrating FortiSandbox with FortiMail .....                          | 113 |
| Connecting FortiSandbox to FortiMail .....                             | 114 |
| Creating an AntiVirus profile .....                                    | 116 |
| Creating a security policy .....                                       | 116 |
| Remote logging in FortiMail using FortiAnalyzer .....                  | 118 |
| Configuring remote logging .....                                       | 118 |
| Securing outbound email from Google Workspace .....                    | 118 |
| Add FortiMail as mail route host in Google Workspace .....             | 119 |
| Route all outbound mail from Google Workspace through FortiMail .....  | 122 |
| Configure access control rule and recipient policy on FortiMail .....  | 125 |
| Using SMTP authentication in FortiMail .....                           | 127 |
| Upgrading FortiMail firmware in HA mode .....                          | 128 |
| Firmware configuration backup .....                                    | 128 |
| HA group firmware upgrade .....                                        | 129 |

# Change Log

| Date       | Change Description |
|------------|--------------------|
| 2024-02-14 | Initial release.   |

# Authentication

This section contains information regarding authentication configurations for FortiMail.

## Microsoft AD Domain Service for FortiMail LDAP profile

This recipe shows how to configure Microsoft Azure Active Directory Domain Services (Azure AD DS) for LDAP authentication with recipient verification on FortiMail.

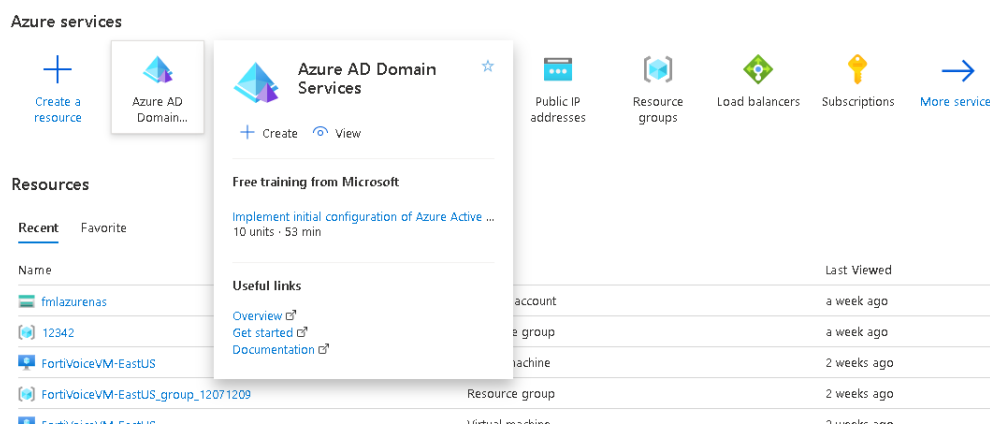


The FortiMail device must operate in either gateway or transparent mode. Server mode is not supported.

## Creating the Azure AD Domain Services instance

Follow the Azure AD Domain Services setup wizard.

1. Go to :  
<https://portal.azure.com/>  
and log in.
2. Either use the navigation menu at the top left corner or search for and select **Azure AD Domain Services**.



3. Select **Create**.
4. Follow the wizard as required, configuring your necessary networking, administration, and synchronization parameters.

5. At the end of the wizard, verify your configuration and select **Create**.

 Microsoft Azure

[Home](#) > [Azure AD Domain Services](#) >

## Create Azure AD Domain Services

\* Basics

\* Networking

Administration

Synchronization

Review + create

Basics

|                |                            |
|----------------|----------------------------|
| Name           | ott-fortivoice.com         |
| Subscription   | Free Trial                 |
| Resource group | OttFortiVoiceResourceGroup |
| Region         | Canada East                |
| SKU            | Enterprise                 |
| Forest type    | User                       |

Network

|                        |                    |
|------------------------|--------------------|
| Virtual network        | (new) aadds-vnet   |
| Subnet                 | (new) aadds-subnet |
| Subnet Address         | 10.0.0.0/24        |
| Network security group | (new) aadds-nsg    |

Administrator group

|                     |                       |
|---------------------|-----------------------|
| Administrator group | AAD DC Administrators |
| Membership Type     | Assigned              |

Notifications

|                                    |     |
|------------------------------------|-----|
| Notify global administrators       | Yes |
| Notify AAD DC administrators group | Yes |

Synchronization

|                       |     |
|-----------------------|-----|
| Synchronization scope | All |
|-----------------------|-----|

Create

Previous

Next

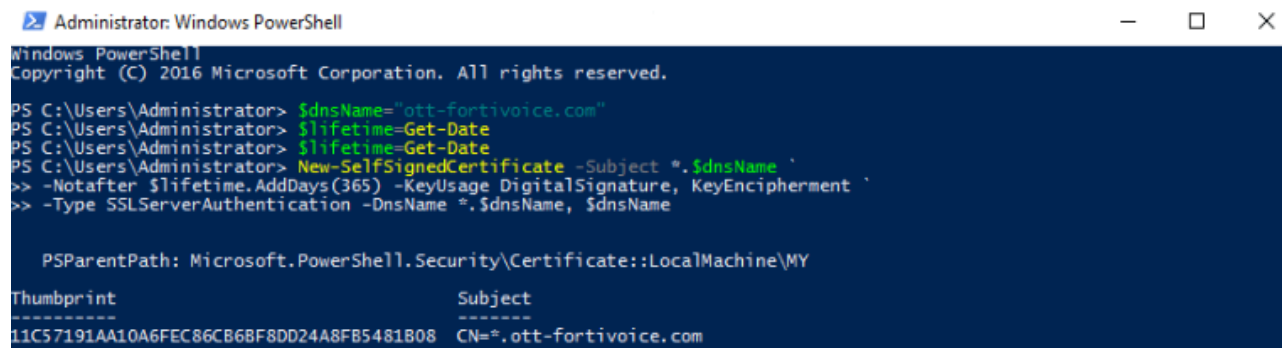
[Download a template for automation](#)

## Enabling Secure LDAP for external access

After the Domain Service instance has been created, you must enable Secure LDAP to allow external access.

1. Generate a self-signed certificate with **SubjectName** as the DNS domain name, making sure that the certificate usage is set correctly.

Below is an example of the PowerShell commands used to create a self-signed certificate.



```

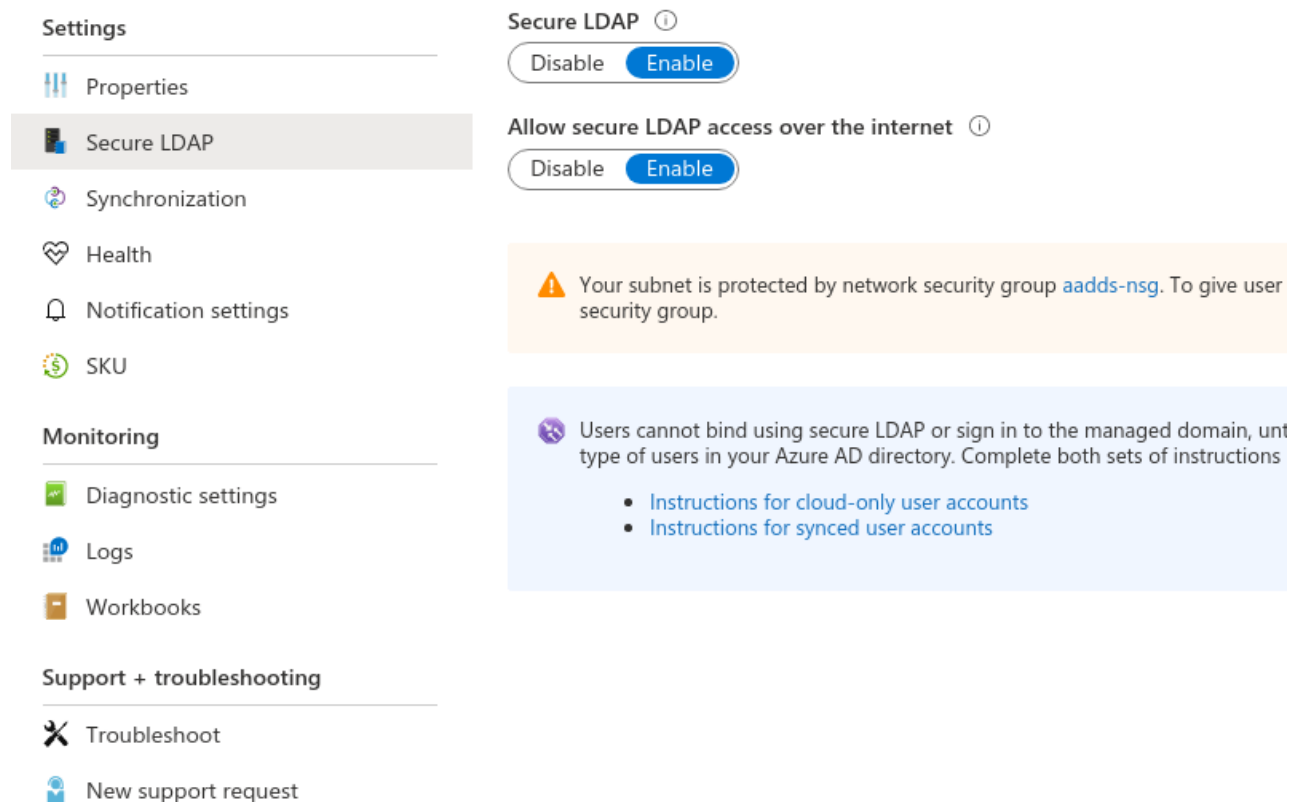
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> $dnsName="ott-fortivoice.com"
PS C:\Users\Administrator> $lifetime=Get-Date
PS C:\Users\Administrator> $lifetime=Get-Date
PS C:\Users\Administrator> New-SelfSignedCertificate -Subject ".$dnsName" `
>> -NotAfter $lifetime.AddDays(365) -KeyUsage DigitalSignature, KeyEncipherment `
>> -Type SSLServerAuthentication -DnsName ".$dnsName, $dnsName

PSParentPath: Microsoft.PowerShell.Security\Certificate::LocalMachine\MY

Thumbprint                                     Subject
-----
11C57191AA10A6FEC86CB68F8DD24A8F85481808    CN=ott-fortivoice.com
  
```

2. Export the self-signed certificate Microsoft Management Console (certificate snap-in) with the private key.
3. In your Domain Service instance in Microsoft Azure, go to **Settings > Secure LDAP**.
4. Enable **Secure LDAP** and **Allow secure LDAP access over the internet**, and then import the certificate.



The screenshot shows the 'Secure LDAP' settings page in the Azure portal. On the left, the 'Settings' menu is visible with options: Properties, Secure LDAP (selected), Synchronization, Health, Notification settings, and SKU. Below this is the 'Monitoring' section with Diagnostic settings, Logs, and Workbooks. At the bottom is 'Support + troubleshooting' with Troubleshoot and New support request. The main content area shows 'Secure LDAP' with an 'Enable' button (the 'Disable' button is greyed out). Below this is 'Allow secure LDAP access over the internet' with an 'Enable' button (the 'Disable' button is greyed out). A yellow warning box states: 'Your subnet is protected by network security group aadds-nsg. To give user security group.' A blue information box states: 'Users cannot bind using secure LDAP or sign in to the managed domain, until type of users in your Azure AD directory. Complete both sets of instructions' with links for 'Instructions for cloud-only user accounts' and 'Instructions for synced user accounts'.

## Adding the Azure AD member to AAD DC Administrator group

After enabling Secure LDAP, you are provided with the external IP address for this service. In the following step, you will edit the network security group to add port 636, to allow external access.

1. In the Domain Service instance, go to **Settings > Properties** and click the name of the security group under **Network security group associated with subnet**.

Search (Ctrl+/) <<

Overview  
Activity log  
Access control (IAM)

**Settings**

**Properties**  
Secure LDAP  
Synchronization  
Health  
Notification settings  
SKU

**Monitoring**

Diagnostics settings  
Logs  
Workbooks

**Support + troubleshooting**

Troubleshoot  
New support request

DNS domain name  
ott-fortivoice.com

Location  
Canada East

SKU  
Enterprise

Forest type  
User

Available in virtual network/subnet  
aadds-vnet/aadds-subnet

Network security group associated with subnet  
**aadds-nsg**

IP address on virtual network  
10.0.0.4 10.0.0.5

Secure LDAP  
Enabled

2. Go to **Settings > Inbound security rules**. Find the security rule named **Port\_636**. Verify that **Action** is set to **Allow**.

Settings

**Inbound security rules**  
Outbound security rules  
Network interfaces  
Subnets  
Properties  
Locks  
Export template  
Monitoring

Inbound security rules

| Priority | Name                          | Port | Protocol | Source                       | Destination    | Action       |
|----------|-------------------------------|------|----------|------------------------------|----------------|--------------|
| 101      | AllowSyncWithAzureAD          | 443  | TCP      | AzureActiveDirectoryDomai... | Any            | Allow        |
| 201      | AllowRD                       | 3389 | TCP      | CorpNetSaw                   | Any            | Allow        |
| 301      | AllowPSRemoting               | 5986 | TCP      | AzureActiveDirectoryDomai... | Any            | Allow        |
| 311      | <b>Port_636</b>               | 636  | TCP      | Any                          | Any            | <b>Allow</b> |
| 65000    | AllowVnetInBound              | Any  | Any      | VirtualNetwork               | VirtualNetwork | Allow        |
| 65001    | AllowAzureLoadBalancerInBound | Any  | Any      | AzureLoadBalancer            | Any            | Allow        |
| 65500    | DenyAllInBound                | Any  | Any      | Any                          | Any            | Deny         |

3. Save changes to the network security group.

4. Go back to **Settings > Properties**. Select a member and add it to the AAD DC Administrator group, and allow it as the bind DN.
5. When finished, log out of Microsoft Azure. Log in as the member you just added, and change the member's password.



This step is necessary in order to make the bind DN work correctly.

## Configuring the FortiMail for recipient address verification

On the FortiMail unit, you must now create an LDAP profile and apply the appropriate DN bind information from your Azure AD Domain Service, and apply it to your domain settings.

1. Log on to the FortiMail admin GUI in either Gateway or Transparent mode.
2. Go to **Profile > LDAP > LDAP** and either click **New** to create a new LDAP profile or edit an existing profile.
3. Enter a **Profile name**, enter the **Server name/IP**, and set **Port** to **636**.
4. Expand **Default Bind Options**, and enter the **Base DN** and **Bind DN** as appropriate.
5. Enter the **Bind password**, and click **Create** or **OK**.

LDAP Profile [ ]

Profile name

Comment

Server name/IP

Port

Fallback server name/IP

Port

Use secure connection

☐ None
 ☒ SSL
 [Test LDAP Query...]

[-] Default Bind Option

Base DN

Bind DN

Bind password

[Browse...]

[+] User Query Option

[+] Group Query Option

☐

[+] User Authentication Option

☒

6. Then go to **Domain & User > Domain > Domain** and either click **New** to create a new protected domain, or edit an existing entry.
7. Expand **Recipient Address Verification**, enable **LDAP Server**, and apply the **LDAP profile** you just configured.

### Recipient Address Verification

LDAP profile

Action on invalid recipient

8. Click **Create** or **OK**.

You can verify that recipient verification works by sending an email and running diagnostics.

```
Trying
Connected to
Escape character is '^]'.
Tue, 7 Jul 2020 04:42:09 +0200
ehlo
250- Hello [172.20.1.124], pleased to meet you
250-ENHANCEDSTATUSCODES
250-PIPELINING
250-8BITMIME
250-SIZE 10485760
250-DSN
250-AUTH LOGIN PLAIN
250-STARTTLS
250-DELIVERBY
250 HELP
mail from:aa@gmail.com
250 2.1.0 aa@gmail.com... Sender ok
rcpt to:bjia@ott-fortivoice.com
250 2.1.5 bjia@ott-fortivoice.com... Recipient ok
rcpt to:adfafd@ott-fortivoice.com
550 5.1.1 <adfafd@ott-fortivoice.com>... User unknown
```

## Microsoft Entra ID as SAML IdP for FortiMail SSO authentication

This recipe shows how to configure Microsoft Entra ID — previously called Azure Active Directory (AD) — as the Security Assertion markup Language (SAML) Identity Provider (IdP) for single sign-on (SSO) authentication on FortiMail.

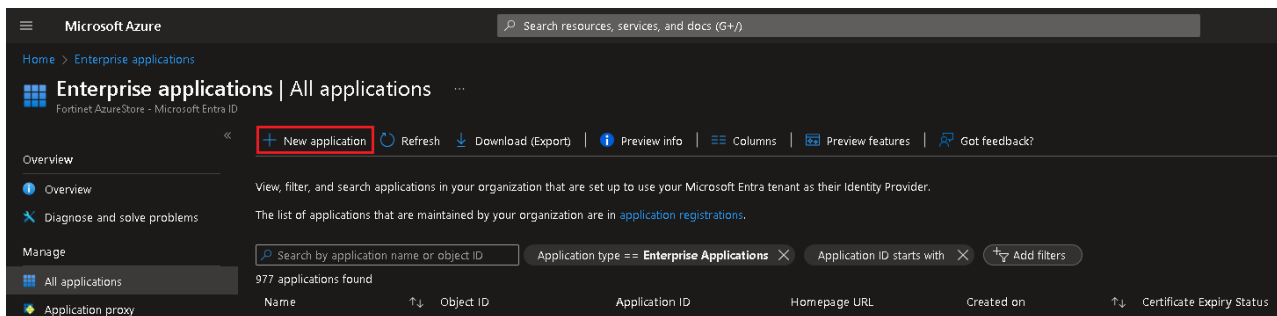
As the IdP, Entra ID receives SSO authentication requests about users from FortiMail. Entra ID then responds to FortiMail with the authentication status.

In this example, DocuSign is the application configured to demonstrate successful SAML SSO user authentication.

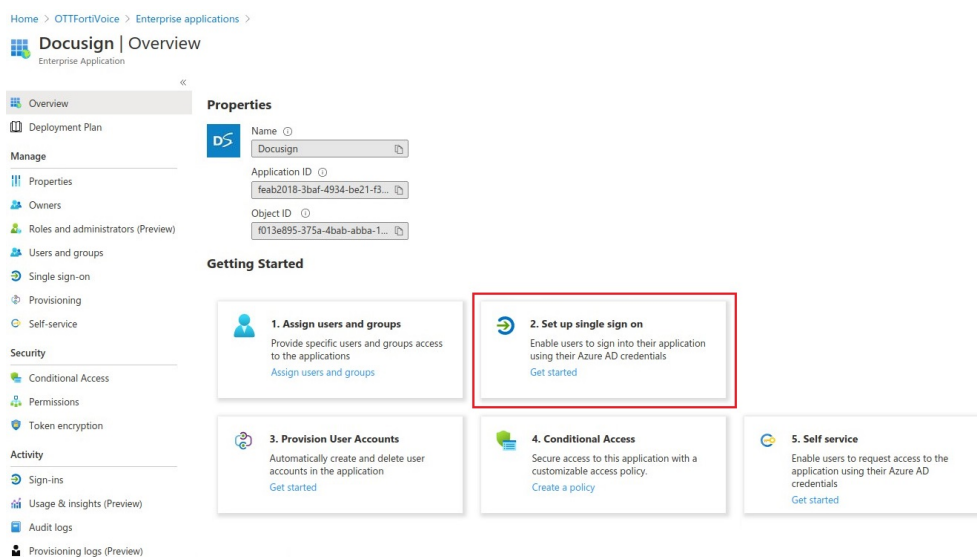
## Configuring Azure AD for SSO with an application

Like other applications, FortiMail also requires that you configure Azure AD if you want it to provide SSO

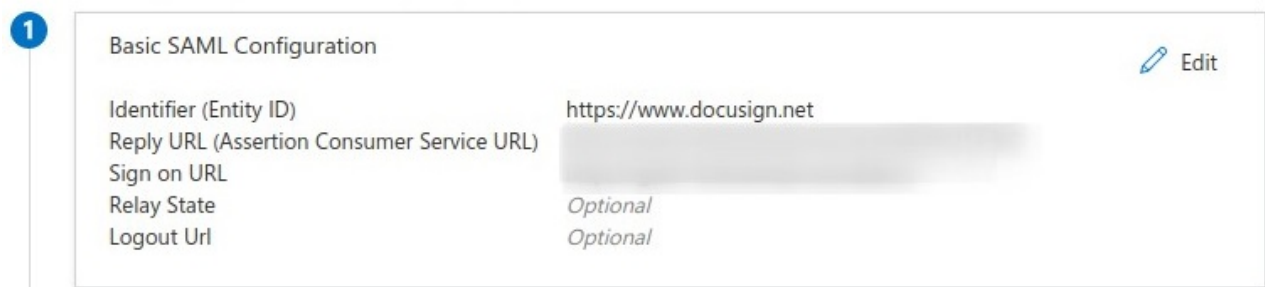
1. Go to :  
<https://portal.azure.com/>  
and log in.
2. To create the DocuSign application, from the Azure Active Directory, from the **Application type** dropdown list, select **Enterprise Applications**. Select **Apply**.



3. Open the application. Select **Set up single sign on** to begin the setup wizard.



4. Configure the settings under **Basic SAML Configuration**, according to the FortiMail device.  
You can find the required **Entity ID** and **ACS URL** in FortiMail under **System > Customization > Single Sign On**. The **Sign on URL** is the SSO landing page URL.



- Configure the **User Attributes & Claims** section.

2

User Attributes & Claims

Edit

|                                   |                        |
|-----------------------------------|------------------------|
| givenname                         | user.givenname         |
| surname                           | user.surname           |
| emailaddress                      | user.mail              |
| name                              | user.userprincipalname |
| urn:oid:0.9.2342.19200300.100.1.3 | user.mail              |
| Unique User Identifier            | user.userprincipalname |

The next step in the setup is necessary for configuring the FortiMail unit. Keep the setup open for the next section of the recipe.

## Configuring SSO on FortiMail

This section configures generates a certificate and configures the secure connection between Azure and FortiMail so that the FortiMail can use SSO to authenticate webmail users.

- In FortiMail, go to **System > Customization > Single Sign On**. Enable SSO for both **Webmail** and **Admin**.

Custom Message

Custom Email Template

Appearance

Single Sign On

Security Fabric

Enabled

Apply to

Webmail

Admin

- From the Azure portal, under **SAML Signing Certificate**, copy the **App Federation Metadata URL**. Then on FortiMail, paste it into the **URL** field under **Identity Provider (IDP) Metadata**.
- Click **Retrieve from URL**. This will populate the IdP metadata **Certificate** field.

3

SAML Signing Certificate

Edit

|                             |                                          |
|-----------------------------|------------------------------------------|
| Status                      | Active                                   |
| Thumbprint                  |                                          |
| Expiration                  | 2/5/2024, 4:46:08 PM                     |
| Notification Email          | @ott-fortivoice.com                      |
| App Federation Metadata Url | https://login.microsoftonline.com/ca8... |
| Certificate (Base64)        | Download                                 |
| Certificate (Raw)           | Download                                 |
| Federation Metadata XML     | Download                                 |

Enabled ☒Apply to ☒ Webmail ☒ Admin**FortiMail Service Provider Metadata**

|              |                                                                                          |
|--------------|------------------------------------------------------------------------------------------|
| Entity ID    | <input type="text" value="https://172.20.34.253/asp"/>                                   |
| Certificate  | <input type="text"/>                                                                     |
| Signature    | <input type="text" value="SHA256"/>                                                      |
| ACS URL      | <input type="text" value="https://172.20.34.253/sso/SAML2/POST"/>                        |
| Metadata URL | <input type="text" value="https://172.20.34.253/sso/Metadata"/> <a href="#">Download</a> |

**Identity Provider (IDP) Metadata**

|      |                                       |                                   |
|------|---------------------------------------|-----------------------------------|
| URL  | <input type="text"/>                  | <a href="#">Retrieve from URL</a> |
| File | <input type="button" value="Upload"/> |                                   |

4. Select **Apply** to enable and finish configuring SSO authentication on the FortiMail unit.  
Users logging into FortiMail can now click **Single Sign On** to be redirected to Azure for authentication.

 Please Login

[Single Sign On](#)

# 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:

Profile name:

Action:

#### Attachment Scan Rules

Total: 6

| Enable...                | File Filter        | Operator | Action      |
|--------------------------|--------------------|----------|-------------|
| <input type="checkbox"/> | executable_windows | Is       | --Default-- |
| <input type="checkbox"/> | video              | Is       | --Default-- |
| <input type="checkbox"/> | audio              | Is       | --Default-- |
| <input type="checkbox"/> | image              | Is       | --Default-- |
| <input type="checkbox"/> | archive            | Is       | --Default-- |
| <input type="checkbox"/> | 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  KB
- ☐ Maximum number of attachment
- ☐ Maximum size   KB
- Action:
- ☒ Adult image analysis
- Action:

---

## Establishing adult image analysis

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

1. Go to **System > FortiGuard > Licensed Feature**.
2. Under **Adult Image Analysis**, click **Enable**.
3. 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.
4. Enter the **Minimum image size** and **Maximum image size** in kilobytes.
5. Click **Apply**.

## 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:

Profile name:

Default action:

### Scan Configurations

|                                                                                  |                                                  |
|----------------------------------------------------------------------------------|--------------------------------------------------|
| <input checked="" type="checkbox"/> <input type="radio"/> FortiGuard             | Action: <input type="text" value="--Default--"/> |
| <input type="radio"/> Greylist                                                   |                                                  |
| <input checked="" type="checkbox"/> <input type="radio"/> SPF                    |                                                  |
| <input type="radio"/> DMARC                                                      | Action: <input type="text" value="--Default--"/> |
| <input type="radio"/> Behavior analysis                                          | Action: <input type="text" value="--Default--"/> |
| <input type="radio"/> Header analysis                                            | Action: <input type="text" value="--Default--"/> |
| <input checked="" type="checkbox"/> <input type="radio"/> Impersonation analysis | Action: <input type="text" value="--Default--"/> |
| <input checked="" type="checkbox"/> <input type="radio"/> Heuristic              | Action: <input type="text" value="--Default--"/> |
| <input type="radio"/> SURBL <a href="#">[Configuration...]</a>                   | Action: <input type="text" value="--Default--"/> |
| <input type="radio"/> DNSBL <a href="#">[Configuration...]</a>                   | Action: <input type="text" value="--Default--"/> |
| <input checked="" type="radio"/> Banned word <a href="#">[Configuration...]</a>  | Action: <input type="text" value="--Default--"/> |
| <input type="radio"/> Safelist word <a href="#">[Configuration...]</a>           |                                                  |
| <input checked="" type="checkbox"/> <input type="radio"/> Dictionary             | Action: <input type="text" value="--Default--"/> |
| <input checked="" type="checkbox"/> <input type="radio"/> Image spam             | Action: <input type="text" value="--Default--"/> |
| <input checked="" type="checkbox"/> <input type="radio"/> Bayesian               | Action: <input type="text" value="--Default--"/> |
| <input type="radio"/> Suspicious newsletter                                      | Action: <input type="text" value="--Default--"/> |
| <input type="radio"/> Newsletter                                                 | Action: <input type="text" value="--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

[+ New...](#) [Delete](#)

« < 1 / 1 > » Records per page: 50 ▼ Total: 1

|   | Banned Word       | Subject                             | Body                                |
|---|-------------------|-------------------------------------|-------------------------------------|
| 1 | You are a winner! | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |

[OK](#) [Cancel](#)

## 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--

+ New...

Edit...

Scan Configurations

+ ☐ FortiGuard

☐ Greylist

+ ☐ SPF

☐ DMARC

☐ Behavior analysis

☐ Header analysis

+ ☐ Impersonation analysis

+ ☐ Heuristic

☐ SURBL [\[Configuration...\]](#)

☐ DNSBL [\[Configuration...\]](#)

☒ Banned word [\[Configuration...\]](#)

☒ Safelist word [\[Configuration...\]](#)

+ ☐ Dictionary

+ ☐ Image spam

+ ☐ Bayesian

☐ Suspicious newsletter

☐ Newsletter

Action: --Default--

Action: --Default--

Action: --Default--

Action: --Default--

Action: --Default--

Action: --Default--

Action: --Default--

Action: --Default--

Action: --Default--

Action: --Default--

Action: --Default--

Action: --Default--

Action: --Default--

Action: --Default--

Action: --Default--

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

## Mitigating spam attacks with weighted analysis profiles

In this recipe, you will configure a weighted analysis profile and define score allocated rules for a variety of identity spoofing attack types that are often used for Business Email Compromise (BEC).

Weighted analysis improves upon the FortiMail device's SPF feature to prevent explicit impersonation attacks. To avoid false positives, weighted analysis balances scan results from multiple attack categories. Each of these categories are assigned a risk score. Based on the particular environment, you may decide to weight certain categories more or less than others, providing a fine-tuned score for your requirements. A targeted attack is detected when the combined score of these categories exceed your custom threshold.

FortiMail 7.4.2 Cookbook  
Fortinet Inc.

23

---

In this example, you will configure a weighted analysis profile that gives more weight to action keywords. Social engineering attacks often use a word or phrase that is a call to action. It tricks users into believing that the email is urgent so that they quickly reply or click a link.

## Creating a dictionary and weighted analysis profile

If you do not have a dictionary profile that defines action keywords in spam, then you must create it first. Otherwise you can skip to the steps to create the weighted analysis profile.

### To configure a weighted analysis profile via the GUI

1. Go to **Profile > Dictionary > Dictionary**.
2. Click **New**.
3. In **Name**, enter a unique name for the dictionary profile.
4. In the **Dictionary Entries** area, click **New**.

Dictionary Profile

Name

custom-call-to-action

Comment

Smart Identifiers

Edit...

Total 6

| Stat... | Type         | Weight | Maximum Weight | Enable Maximum ... | Scan Area    |
|---------|--------------|--------|----------------|--------------------|--------------|
| ✖       | Canadian SIN | 1      | 1              | ✔                  | Header; Body |
| ✖       | US SSN       | 1      | 1              | ✔                  | Header; Body |
| ✖       | Credit Card  | 1      | 1              | ✔                  | Header; Body |
| ✖       | ABA Routing  | 1      | 1              | ✔                  | Header; Body |
| ✖       | CUSIP        | 1      | 1              | ✔                  | Header; Body |
| ✖       | ISIN         | 1      | 1              | ✔                  | Header; Body |

Dictionary Entries

New...

Edit...

Delete

1 / 1

Records per page 50

Total 2

| Stat... | Pattern         | Type  | Weight | Maximum Weig... | Enable Maximu... | Scan Area    |
|---------|-----------------|-------|--------|-----------------|------------------|--------------|
| ✔       | pr[0o]p[0o]sal  | Regex | 1      | 1               | ✖                | Header; Body |
| ✔       | limited[-]*time | Regex | 1      | 1               | ✖                | Header; Body |

OK

Cancel

In **Pattern type**, select **Regex**.

In **Pattern**, enter a regular expression that matches a call-to-action word that you usually see in spam, but do not see in normal email. Click **Validate** to test that your regular expression matches spam text, but not similar normal text.

For example:

`pr[0o]p[0o]sal`

matches the word "proposal", even if attackers substitute the letter O with the number 0 in order to try to evade detection. For more examples and regular expression syntax, see the [FortiMail Administration Guide](#).

Click **Create**.

Repeat this step for every call-to-action word or phrase that you want to match, and then click **Create**.

5. Go to **Profile > AntiSpam > Weighted Analysis**.

6. Click **New**.

7. From **Domain**, select whether the profile will be system-wide or apply to a specific protected domain.

8. In **Name**, enter a unique name for the weighted analysis profile.
9. In the **Rule** area, click **New**.

Weighted Analysis Profile

Domain

--System--

Name

custom-weighted-profile

Comment

Rule

+ New...

Edit...

Delete

Move

1

/ 1

Records per page

50

Total: 0

| Status | Name | Action |
|--------|------|--------|
|--------|------|--------|

CreateCancel

In **Name**, enter a unique name for the rule.

From **Action**, select what FortiMail should do when this rule detects spam.

In the **Score Weight** area, set **Action keyword** to **20**. This increases the score for emails that contain action keywords, which increases the probability that the email will be detected as spam. In **Dictionary profile**, select the dictionary profile that you created in previous steps.

Rule

Status 

Name

Action 

--Default--

+

Threshold 

50

Score Weight

Intelligent analysis 

50

Cousin domain 

10

Suspicious character 

10

Sender alignment 

10

Action keyword 

20

Dictionary profile 

custom-call-to-action

+

New...

Minimum dictionary score 

1

URL category 

10

URL profile 

unrated

+

Malformed email 

10

Create

Cancel

Click **Create**, and then click **Create**.

- Later, when testing your configuration, if the rule is too sensitive and accidentally detects non-spam (false positives), then return to this rule. Either reduce the **Action keyword** score or increase **Threshold**. This provides granular control.



**Threshold** must be equal or less than the total of all categories in the **Score Weight** area. Otherwise, even if an email matches all spam categories, it still will not meet the threshold, and the action will never be triggered.

### To configure a weighted analysis profile via the CLI

```

config profile dictionary
  edit custom-call-to-action
    config item
      edit 0
        set pattern "pr[0o]p[0o]sal"
      next
    end
  next
end
config profile weighted-analysis
  edit custom-weighted-profile
    config rule
      edit 1
        set name custom-weighted-rule
        set action-keyword-score 20.000000
        set dictionary-profile custom-call-to-action
      next
    end
  end
end

```

```
end
next
end
```

## Assigning the weighted analysis profile to the antispam profile

If you already have antispam profiles, you can select the weighted analysis profile there in order to apply it. Otherwise follow the example below to create a new antispam profile.

### To apply a weighted analysis profile in an antispam profile via the GUI

1. Go to **Profile > AntiSpam > AntiSpam**.
2. Click **New**, or select and **Edit** an existing profile.  
For this example, we edit AS\_Inbound, a profile that is applied to all inbound traffic.
3. In the **Scan Configurations** area, enable and expand **Business email compromise** and **Weighted analysis**.
4. From **Profile**, select the weighted analysis profile that you created [in previous steps](#).

The screenshot shows the 'AntiSpam Profile' configuration window. At the top, there are fields for 'Domain' (set to '--System--'), 'Name' (set to 'AS\_Inbound'), and 'Comment'. Below these is a 'Default action' dropdown set to '--None--'. The 'Scan Configurations' section is expanded, showing a list of scanning engines. 'FortiGuard', 'SPF', 'DMARC', and 'Weighted analysis' are enabled (indicated by green circles). 'Weighted analysis' is expanded, showing a 'Profile' dropdown set to 'custom-weighted-profile'. Other scanning engines like 'Greylist', 'DKIM', 'ARC', 'Behavior analysis', 'Header analysis', 'Impersonation analysis', 'Cousin domain', and 'Sender alignment' are disabled. Each scanning engine has an 'Action' dropdown set to '--Default--'. At the bottom right, there are 'Create' and 'Cancel' buttons.

5. Click **Create** or **OK**.

### To apply a weighted analysis profile in an antispam profile via the CLI

```
config profile antispam
```

---

```
edit AS_Inbound
    set weighted-analysis-status enable
    set weighted-analysis-profile custom-weighted-profile
end
```

## Configuring the inbound policy for weighted analysis

If you already have policies, you can select the antispam profile there in order to apply the weighted analysis profile that it references. Otherwise follow the example below to create a new policy.

Once these steps are complete, all incoming emails will be checked for all weighted analysis categories, with a greater emphasis for those emails containing action keywords. Emails that trigger the configured threshold are caught and dealt with according to your selected **Action**.

### To apply an antispam profile in a policy via the GUI

1. Go to either **Policy > IP Policy > IP Policy** or **Policy > Recipient Policy > Inbound**.
2. Click **New**, or edit an existing policy.  
For this example, edit the IP-based policy for all incoming and outgoing traffic.
3. Expand the **Profiles** section. From **AntiSpam**, select the **AS\_Inbound** antispam profile that you configured earlier.

IP Based Policy

Status
☒

Source
IP/Netmask
0.0.0.0
/
0

Destination
IP/Netmask
0.0.0.0
/
0

Action
Scan

Comment

Profiles

Session
Inbound\_Session
+

AntiSpam
AS\_Inbound
+

AntiVirus
AV\_SysQuarantine
+

Content
--None--
+

DLP
--None--
+

IP pool
--None--
+

+
Authentication and Access

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

OK
Cancel

Optionally, expand the **Miscellaneous** section and enable **Take precedence over recipient based policy match**.

4. Click **OK**.

#### To apply an antispam profile in a policy via the CLI

```
config policy ip
edit <policy_int>
set profile-antispam AS_Inbound
set exclusive enable
end
```

## 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                | <input checked="" type="checkbox"/>                                 |
| Sender pattern:        | <div>User Defined</div> <div>██████@fortinet.com</div>              |
| Recipient pattern:     | <div>User Defined</div> <div>*</div>                                |
| Sender IP/netmask:     | <div>User Defined</div> <div>192.168.200.0/24</div>                 |
| Reverse DNS pattern:   | <div>*</div> <div><input type="checkbox"/> Regular Expression</div> |
| Authentication status: | <div>Any</div>                                                      |
| TLS profile:           | <div>--None--</div> <div>+ New... Edit...</div>                     |
| Action:                | <div>Reject</div>                                                   |
| Comments:              | <div></div>                                                         |

Create Cancel

## 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 identity 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--  + New...  Edit...

☐ **Enable PKI authentication for webmail access** --None-- 

☐ **Certificate validation is mandatory**

---

**OK**

Cancel

## 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

+ New...

Edit...

☐ Include original message as attachment

Create

Cancel

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

FortiMail

Please specify name:

oversized

OK

Cancel

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

Nameoversized

TypeGeneric

Description:

Subject:Oversized Message from %%ORIG\_ENVELOPE\_FROM%% has been sent to quaraiInsert Variables...

From:%%NOTIFY\_FROM%%Insert Variables...

To:%%NOTIFY\_TO%%Insert Variables...

Envelope from:%%NOTIFY\_FROM%%Insert Variables...

Envelope to:%%ORIG\_ENVELOPE\_TO%%Insert Variables...

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%%

Insert Variable...

Insert Color Co...

Preview

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

Insert Variable...

Reset to Default

OKCancel

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:

Profile name:

☐ Tag subject

☐ Insert header

☐ Insert disclaimer  at

☐ Deliver to alternate host

☐ Deliver to original host

☐ BCC

☐ Replace with message:

☐ Archive to account

☒ Notify with profile

☒ Final action:

Create

Cancel

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:

OK

Cancel

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  KB
- ☐ Maximum number of attachment
- ☒ Maximum size   KB
  - Action:
- ☐ Adult image analysis
  - Action:

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:        | <input type="text" value="3"/>      |
| Restrict number of email per session to:             | <input type="text" value="10"/>     |
| Restrict number of recipients per email to:          | <input type="text" value="500"/>    |
| Cap message size (KB) at:                            | <input type="text" value="204800"/> |
| Cap header size (KB) at:                             | <input type="text" value="32"/>     |
| Maximum number of NOOPs allowed for each connection: | <input type="text" value="10"/>     |
| Maximum number of RSETs allowed for each connection: | <input type="text" value="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:

Profile name:

Default action:

### Scan Configurations

☒ FortiGuard

Action:

☐ Greylist

☒ **SPF**

☒ Fail

Action:

☒ Soft Fail

Action:

☐ Sender Alignment

Action:

☐ Permanent Error

Action:

☐ Temporary Error

Action:

☐ Pass

Action:

☐ Neutral

Action:

☐ None

Action:

### 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: | <input type="text" value="1200"/> |
| Restrict the number of messages per client per 30 minutes to:    | <input type="text" value="0"/>    |
| Restrict the number of recipients per client per 30 minutes to:  | <input type="text" value="0"/>    |
| Maximum concurrent connections for each client:                  | <input type="text" value="2"/>    |
| Connection idle timeout (seconds):                               | <input type="text" value="30"/>   |

### Sender Reputation

### Endpoint Reputation

### Sender Validation

SPF check:  

- ☐ 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:

 New...

 Edit...

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-- ▼ + New...  Edit...

### 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.

## DKIM Setting

+ New... Delete Download Activate

Refresh « < 1 / 1 > » Records per page: 50 Selected: 1 / 1

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

Close

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--

+ New...

Edit...

Scan Configurations

+ FortiGuard

Action: --Default--

Greylist

+ SPF

Action: Discard\_Inbound

DMARC

FortiMail 7.4.2 Cookbook  
Fortinet Inc.

46

## 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**.

|         |           |                 |                |                |
|---------|-----------|-----------------|----------------|----------------|
| License | AntiVirus | <b>AntiSpam</b> | URI Protection | GeoIP Override |
|---------|-----------|-----------------|----------------|----------------|

---

**FortiGuard AntiSpam Options**

|                                  |                                     |
|----------------------------------|-------------------------------------|
| Enable service                   | <input checked="" type="checkbox"/> |
| FortiGuard server port:          | 8888 ▼                              |
| FortiGuard server protocol:      | UDP ▼                               |
| Spam outbreak protection:        | Low ▼                               |
| Spam outbreak protection period: | 30 (Minutes)                        |
| Use override server:             | <input checked="" type="checkbox"/> |
| Override server address:         | 10.180.164.122 + -                  |
| Enable cache                     | <input checked="" type="checkbox"/> |
| Cache TTL (Seconds):             | 300 (300~1800)                      |
| Server location:                 | US only <b>Any location</b>         |

**Apply** **Update Now** **Cancel**

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:

Profile name:

Default action:

+ New...

Edit...

Scan Configurations

FortiGuard

Action:

+ IP Reputation

URI filter

Primary

Secondary

Spam outbreak protection

Action:

Action:

Action:

## 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--



+ New...

Edit...

AntiSpam:

fortiguard-antispam



+ New...

Edit...

AntiVirus:

--None--



+ 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

Create

Cancel

## 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**.

License

AntiVirus

AntiSpam

URI Protection

---

FortiGuard AntiVirus Options

Use override server address

☐

Override server address:

+ -

Allow push update

☒

Use override push IP

☐

Virus outbreak protection:

Virus outbreak protection period:

(Minutes)

Virus database:

Scheduled update

☒

(hour)

Apply

Update Now

Cancel

## 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 + New... Edit...

☒ AntiVirus

☒ Malware/virus outbreak

Action: --Default-- + New... Edit...

☒ Heuristic

Action: --Default-- + New... Edit...

☐ File signature check

Action: --Default-- + New... Edit...

☒ Grayware

☐ FortiSandbox

Scan mode: Submit and wait for result Submit only

☐ Attachment analysis

Malicious/Virus

Action: --Default-- + New... Edit...

High risk

Action: --Default-- + New... Edit...

Medium risk

Action: --Default-- + New... Edit...

Low risk

Action: --Default-- + New... Edit...

No Result

Action: --None-- + New... Edit...

☐ URL analysis

Malicious/Virus

Action: --Default-- + New... Edit...

High risk

Action: --Default-- + New... Edit...

Medium risk

Action: --Default-- + New... Edit...

Low risk

Action: --Default-- + New... Edit...

No Result

Action: --None-- + New... Edit...

Create Cancel

## 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:   /

Destination:   /

Action:

Comment:

#### Profiles

|            |                                                   |                                         |                                        |
|------------|---------------------------------------------------|-----------------------------------------|----------------------------------------|
| Session:   | <input type="text" value="--None--"/>             | <input type="button" value="+ New..."/> | <input type="button" value="Edit..."/> |
| AntiSpam:  | <input type="text" value="--None--"/>             | <input type="button" value="+ New..."/> | <input type="button" value="Edit..."/> |
| AntiVirus: | <input type="text" value="fortiguard-antivirus"/> | <input type="button" value="+ New..."/> | <input type="button" value="Edit..."/> |
| Content:   | <input type="text" value="--None--"/>             | <input type="button" value="+ New..."/> | <input type="button" value="Edit..."/> |
| DLP:       | <input type="text" value="--None--"/>             | <input type="button" value="+ New..."/> | <input type="button" value="Edit..."/> |
| IP pool:   | <input type="text" value="--None--"/>             | <input type="button" value="+ New..."/> | <input type="button" value="Edit..."/> |

#### Authentication and Access

Authentication type:

#### Miscellaneous

☐ Reject different SMTP sender identity for authenticated user

☐ Sender identity verification with LDAP server for authenticated user

LDAP profile:

☐ Take precedence over recipient based policy match

Create

Cancel

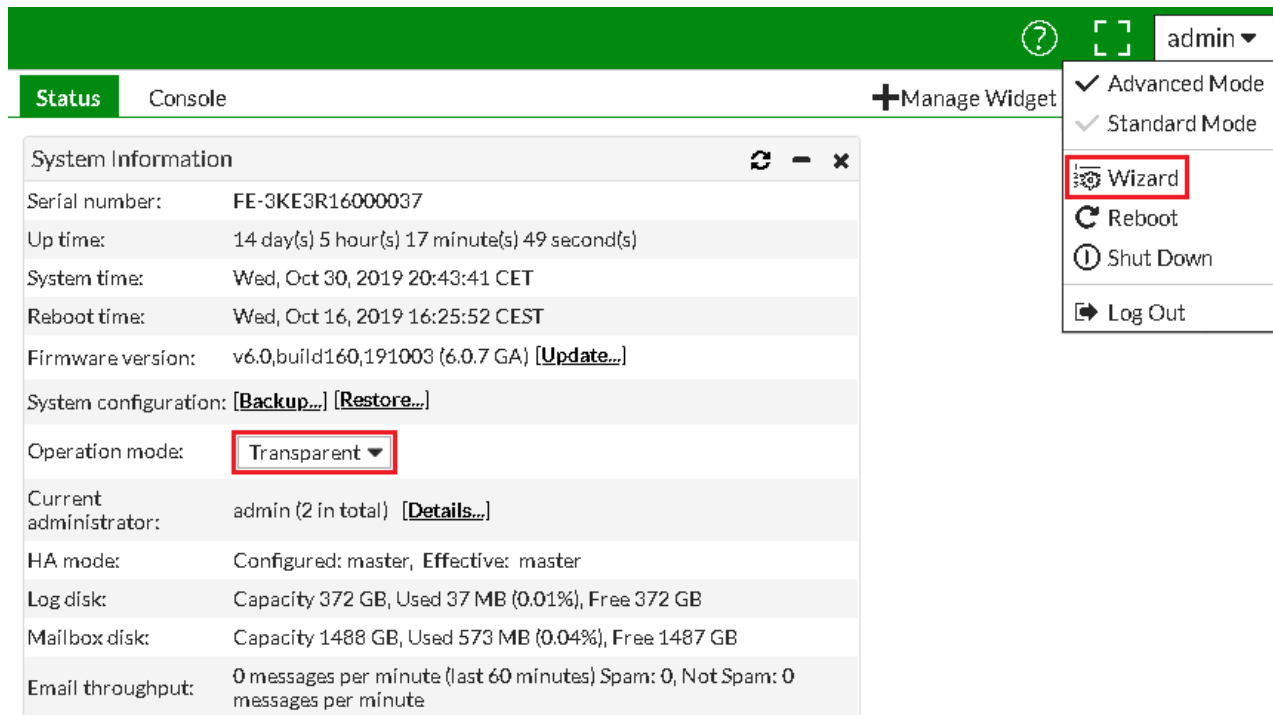
## Preventing an ISP from being blocklisted

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.



### 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:  /

IPv6/Netmask:  /

Advanced Setting

Access:

HTTPS

PING

SSH

SNMP

HTTP

TELNET

Web access:

Admin

Webmail

Mail access:

POP3

IMAP

POP3S

IMAPS

MTU:

Administrative status: 

Up

Down

SMTP Proxy

OK

Cancel

## 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:

### Connection Settings

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

### Sender Reputation

- Enable sender reputation ☒
- Throttle client at:
- Restrict number of email per hour to:
- Restrict email to:  percent of previous hour
- Temporarily fail client at:
- Reject client at:
- FortiGuard IP reputation check:

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:  

Message selection:  

- ☐ 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   
- ☐ 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  / 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

Create

Cancel

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.

Mapping can be either:

- **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:

Domain:

**Impersonation**

**Match Rule** **Exempt Rule**

New...

Edit...

Delete

/

Records per page:  Total: 0

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

Create

Cancel

## 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):

The screenshot shows the MXToolbox SuperTool interface. The 'DNS Lookup' tab is selected. The domain 'fortinet.com' is entered, and the 'SPF Record Lookup' button is clicked. The results show the SPF record for 'spf:fortinet.com' as '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'. Below the record, a table provides details for each IP range.

| 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. |

TOOLBOX

SuperTool

MX Lookup

Blacklists

DMARC

Diagnostics

Email Health

DNS Lookup

Analyze Headers

SuperTool Beta7

fortinet.com dkim

DKIM Lookup

dkim:fortinet.com:dkim

Find Problems

dkim

k=rsa; p=MIIBIjANBgkqhkiG9w0BAQFAAQCAQEAQAEwXjJl+pvOzLslANCffq950R8J2SQ04p8ZLVtWJMcK3aJouyYTN6UkhCkZELfXHZL3O6nUDz+mx14f/7471g5wB1bFzcn1a6DAYYNNeyr2nvHepObVjrqLNTIB59yqkOzrOxt9b1CXhV77Tb2OoR4NrcXknCO1XBthF5McDygc2mx/SPV10S1YPEADA7nPvZqyORTTuOxdBAXYSvew1/Q/R476KBqPeX1YMOx5Qq56jSISjSgF2j3cQBqVf7bIHgNZ7PFGa6sqPnzSqnP6kU2n81QurAXR6CoXfFn78vvZzgN7hKKQoeIFx61IgmOhdReixnRtTwq7C19vxMVpv3wIDAQAB

| Tag | TagValue                                                                                                                                                                                                                                                                                                                                                                                     | Name       | Description                                                                                          |
|-----|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|------------------------------------------------------------------------------------------------------|
| k   | rsa                                                                                                                                                                                                                                                                                                                                                                                          | Key Type   | The type of the key used by tag (p).                                                                 |
| p   | MIIBIjANBgkqhkiG9w0BAQFAAQCAQEAQAEwXjJl+pvOzLslANCffq950R8J2SQ04p8ZLVtWJMcK3aJouyYTN6UkhCkZELfXHZL3O6nUDz+mx14f/7471g5wB1bFzcn1a6DAYYNNeyr2nvHepObVjrqLNTIB59yqkOzrOxt9b1CXhV77Tb2OoR4NrcXknCO1XBthF5McDygc2mx/SPV10S1YPEADA7nPvZqyORTTuOxdBAXYSvew1/Q/R476KBqPeX1YMOx5Qq56jSISjSgF2j3cQBqVf7bIHgNZ7PFGa6sqPnzSqnP6kU2n81QurAXR6CoXfFn78vvZzgN7hKKQoeIFx61IgmOhdReixnRtTwq7C19vxMVpv3wIDAQAB | 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 |

TOOLBOX

SuperTool

MX Lookup

Blacklists

DMARC

Diagnostics

Email Health

DNS Lookup

Analyze Headers

SuperTool Beta7

fortinet.com

DMARC Lookup

dmARC:fortinet.com

Find Problems

Solve Email Delivery Problems

dmARC

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' separated 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.

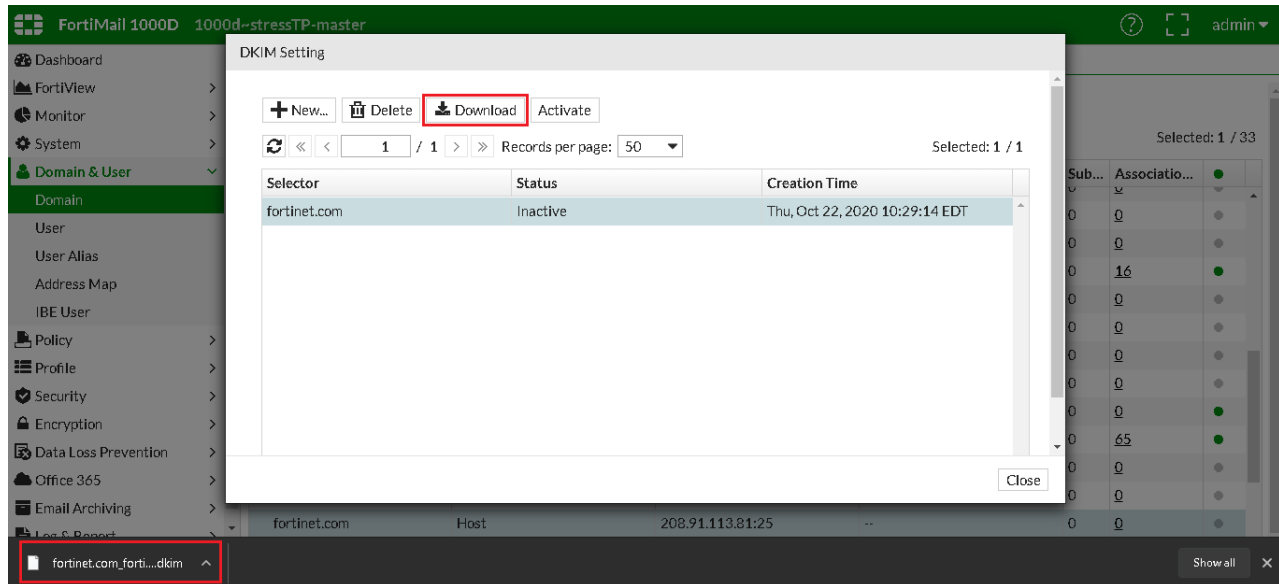
For more information about these email authentication protocols, see the [FortiMail Administration Guide](#). For a recipe regarding email checking, see [Configuring incoming email DMARC checking with SPF and DKIM](#).

## 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.



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](https://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/KlS60mBBYKjl+gpL0jPAE+zYYlpa0mLLm6b01NReZ+BXBoX2fldQ8xUkcMcEYz6ficlvvOZwTug=
="
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/7471gSwBibFzcnla6DAYYNNEYr2nvHepObVjrqlMTIB59yqkOzrOxt
9biCXhV77TbZOoR4NrCxnC"
"OixBthFSMcDyqc2mx/SPvi0SiYPeADA7nPVZqy0RTTuOxdbAxYSvewi/Q/R476KBqnPeXLYMOr5OqS6jSISjSgF2
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

---

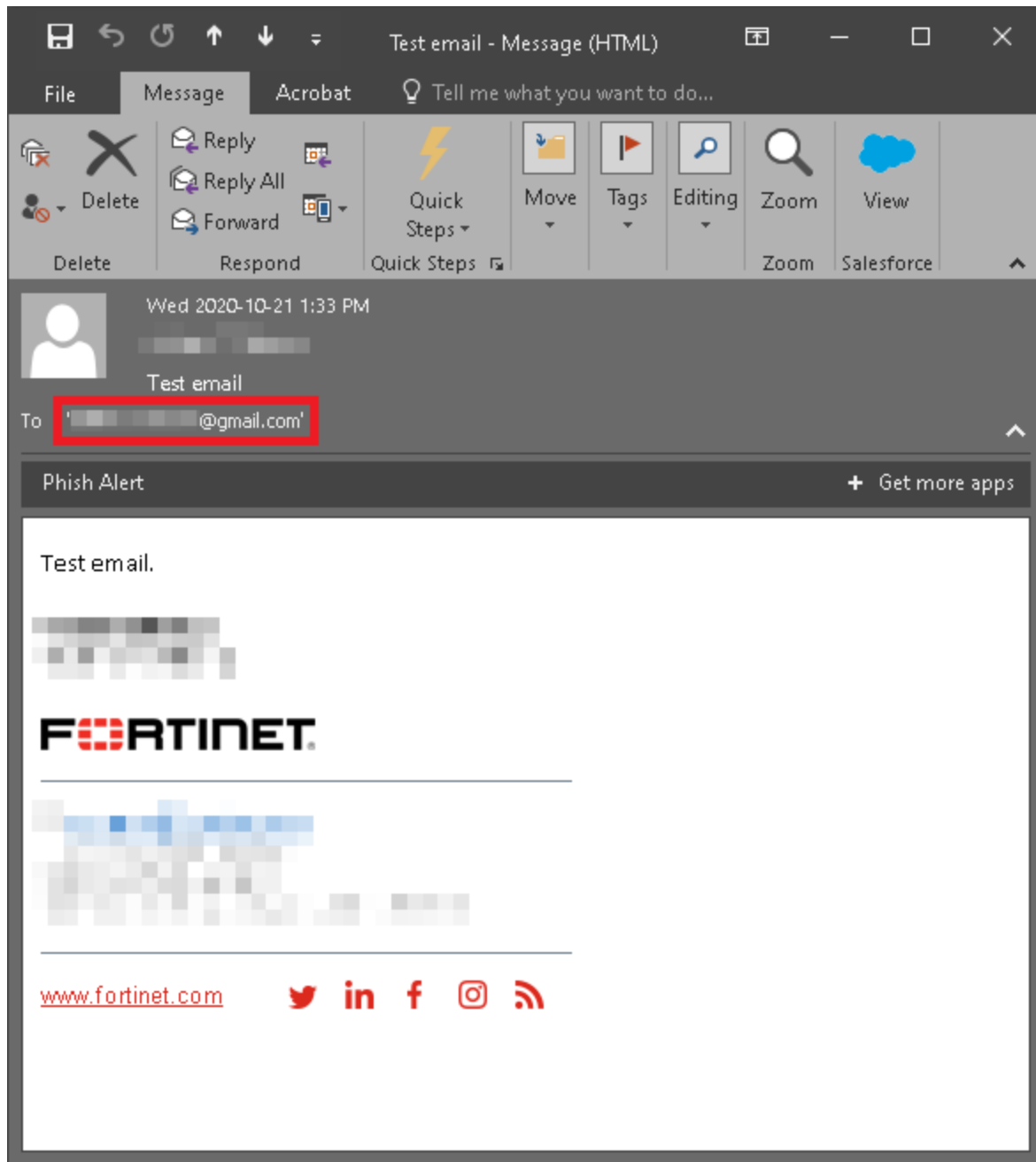
and DKIM feedback.

```
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
```

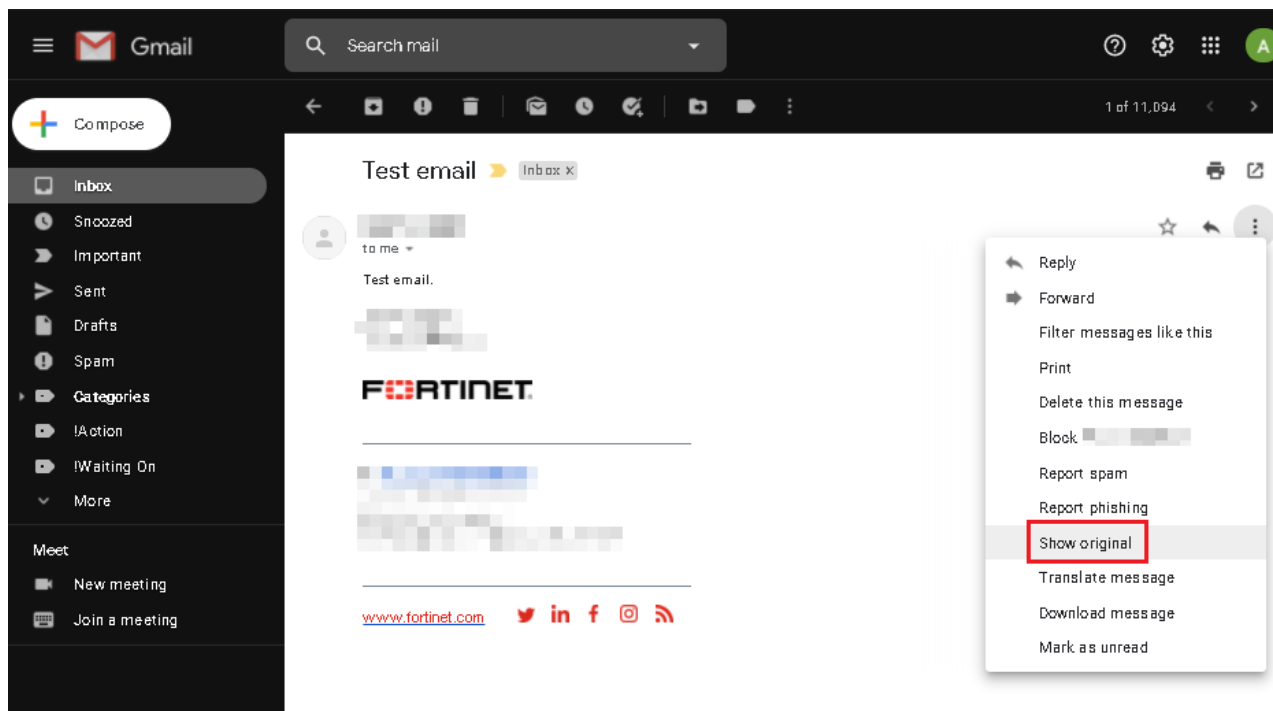
## Testing email signing and verification

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.



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] <a href="#">Learn more</a>         |
| DKIM:       | 'PASS' with domain fortinet.com <a href="#">Learn more</a> |
| DMARC:      | 'PASS' <a href="#">Learn more</a>                          |

[Download original](#)

[Copy to clipboard](#)

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 FortiMail.

## 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

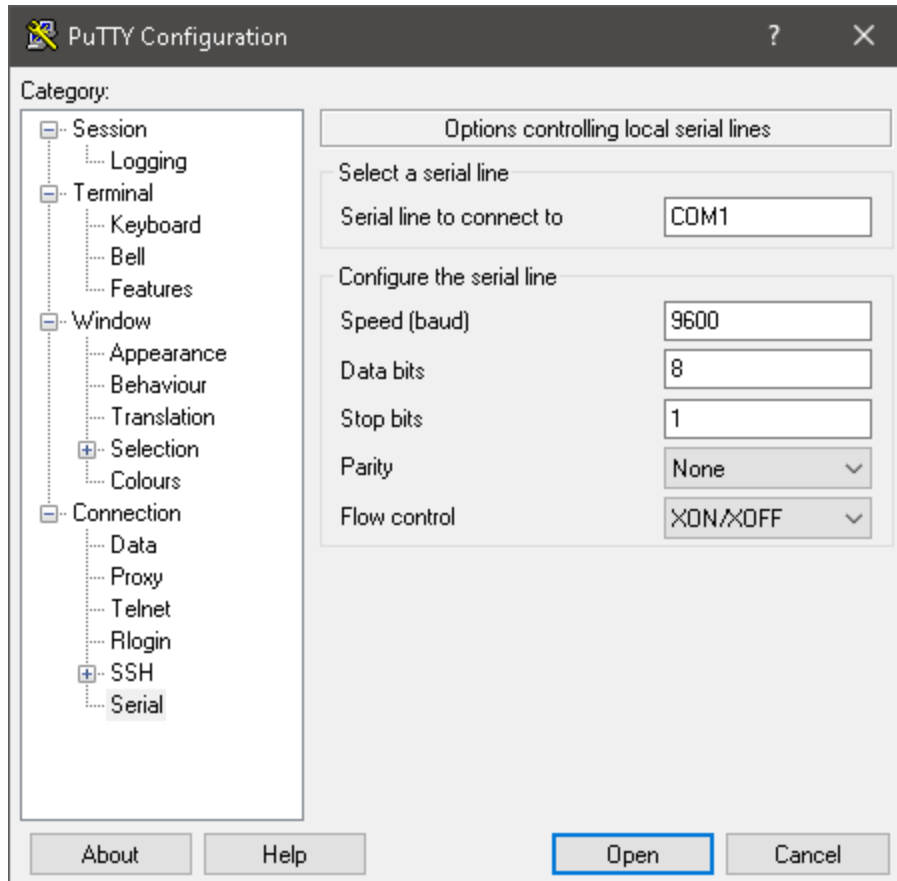
## Physically connect the FortiMail unit

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**.



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
```

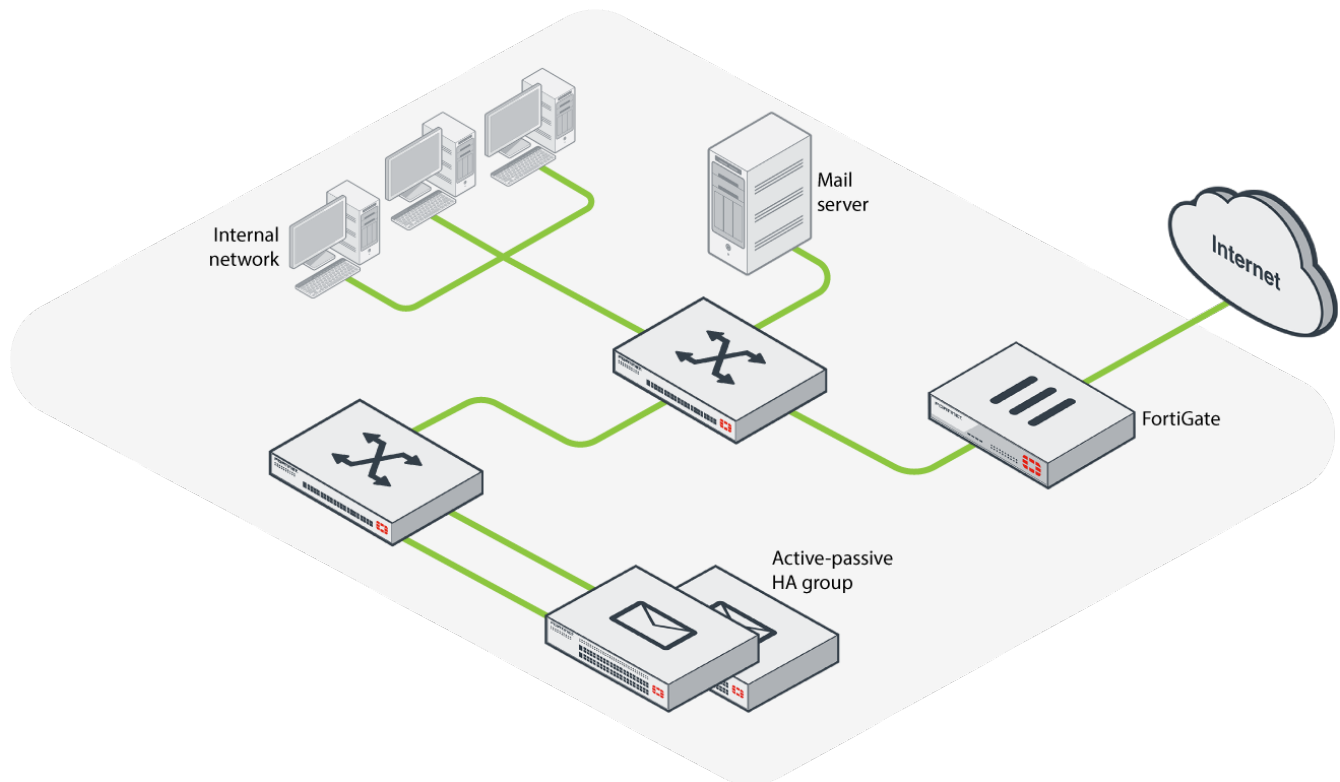
If the administrator account has somehow been deleted, enter the following command to reset the FortiMail unit to its factory default configuration:

```
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**.

Status

Configuration

HA Configuration

Mode of operation: master

On failure: wait for recovery then restore slave slave role

Shared password: \*\*\*\*\*

Advanced options

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.

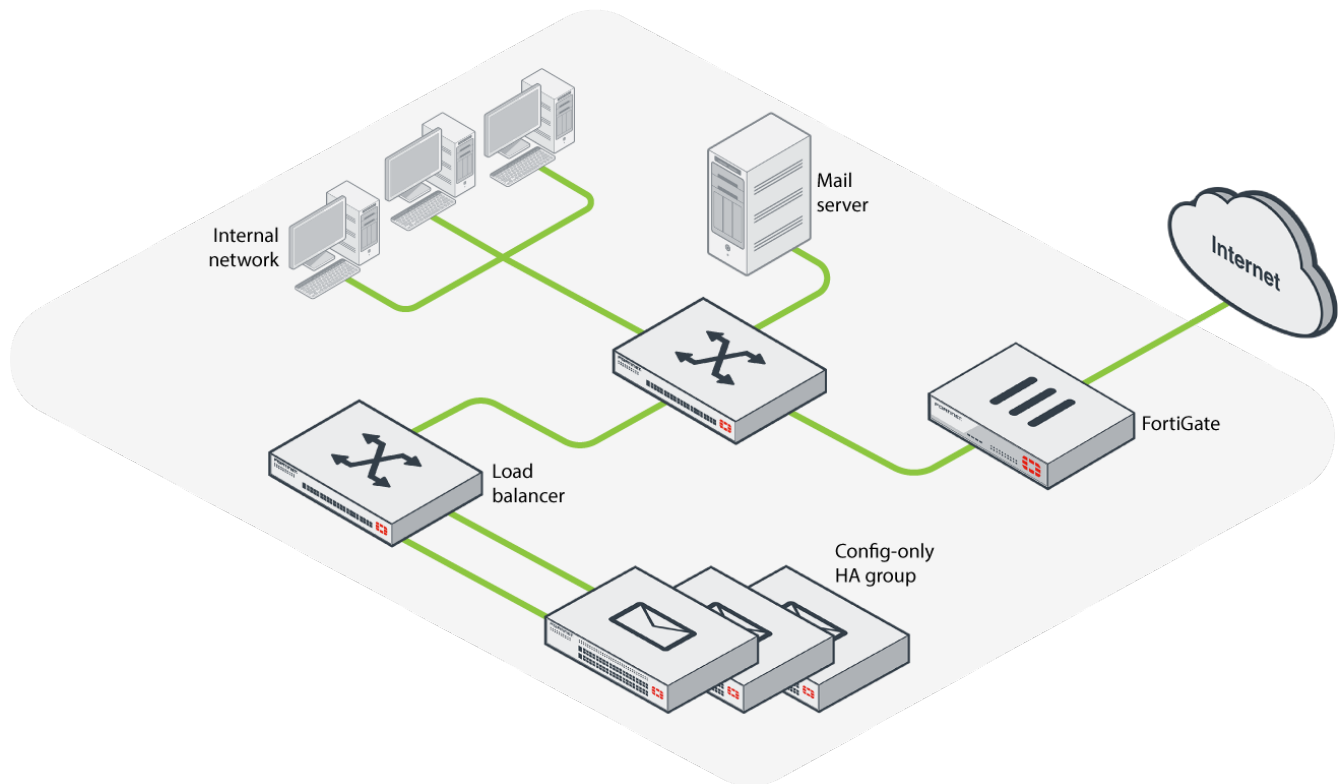
---

## Restoring from a backup

The **Restore Options** area of the Mail Data tab lets you selectively restore email users' mailboxes from mailbox backups. The restored mailboxes will be merged with the current mailboxes.

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.
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**.

Mail Server Settings

Relay Host List

Disclaimer

Disclaimer Exclusion List

Storage

Proxies

Option

Local

NAS

Protocol:

NFS

Test...

Hostname/IP address:

Port:

2049

Directory:

/var/nfs

Centralized Quarantine

Disabled

Receive quarantined messages from clients

Send quarantined messages to remote server

Client IP:

+

Centralized IBE

Disabled

Receive IBE messages from clients

Send IBE messages to remote server over SSL

Client IP:

+

Apply

Cancel

## 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**.

Status

Configuration

HA Configuration

Mode of operation: config master

Shared password: \*\*\*\*\*

Advanced options

HA base port: 20000

+ Create

🗑 Delete

Total: 1

IP address

192.168.1.1

Apply

Cancel



## 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 your 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](https://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

Create

Cancel

## 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 your 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                          | <input checked="" type="checkbox"/>                    |
| IBE service name:                           | <input type="text" value="Identity Based Encryption"/> |
| User registration expiry time (days):       | <input type="text" value="30"/>                        |
| User inactivity expiry time (days):         | <input type="text" value="90"/>                        |
| Encrypted email storage expiry time (days): | <input type="text" value="180"/>                       |
| Password reset expiry time (hours):         | <input type="text" value="24"/>                        |
| Allow secure replying                       | <input checked="" type="checkbox"/>                    |
| Allow secure forwarding                     | <input checked="" type="checkbox"/>                    |
| Allow secure composing                      | <input checked="" type="checkbox"/>                    |
| IBE base URL:                               | <input type="text" value="https://172.20.143.94"/>     |
| "Help" content URL:                         | <input type="text" value="https://172.20.143.94"/>     |
| "About" content URL:                        | <input type="text" value="https://172.20.143.94"/>     |
| Allow custom user control                   | <input type="checkbox"/>                               |

### Notification Settings

- ☒ Send notification to sender when message is read [Edit...](#)
- ☒ Send notification if message remains unread for  day(s)
- ☐ Notification to sender [Edit...](#)
- ☒ Notification to recipient [Edit...](#)

Apply

Cancel

## 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:                      | <input type="text" value="confidential-encryption"/> |
| Protocol:                          | <input type="text" value="IBE"/>                     |
| Access method:                     | <input type="text" value="Push"/>                    |
| Maximum size (KB) for Push method: | <input type="text" value="1024"/>                    |
| Encryption algorithm:              | <input type="text" value="AES 128"/>                 |
| Action:                            | <input type="text" value="Encrypt"/>                 |
| Action on failure:                 | <input type="text" value="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                          | <input checked="" type="checkbox"/>                    |
| IBE service name:                           | <input type="text" value="Identity Based Encryption"/> |
| User registration expiry time (days):       | <input type="text" value="30"/>                        |
| User inactivity expiry time (days):         | <input type="text" value="90"/>                        |
| Encrypted email storage expiry time (days): | <input type="text" value="180"/>                       |
| Password reset expiry time (hours):         | <input type="text" value="24"/>                        |
| Allow secure replying                       | <input checked="" type="checkbox"/>                    |
| Allow secure forwarding                     | <input type="checkbox"/>                               |
| Allow secure composing                      | <input type="checkbox"/>                               |
| IBE base URL:                               | <input type="text" value="https://172.20.140.203"/>    |
| "Help" content URL:                         | <input type="text"/>                                   |
| "About" content URL:                        | <input type="text"/>                                   |
| Allow custom user control                   | <input type="checkbox"/>                               |

### Notification Settings

- ☐ Send notification to sender when message is read [Edit...](#)
- ☐ Send notification if message remains unread for  day(s)
- ☐ Notification to sender [Edit...](#)
- ☐ Notification to recipient [Edit...](#)

Apply

Cancel

## 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:                      | <input type="text" value="IBE-push"/>          |
| Protocol:                          | <input type="text" value="IBE"/>               |
| Access method:                     | <input type="text" value="Push"/>              |
| Maximum size (KB) for Push method: | <input type="text" value="1024"/>              |
| Encryption algorithm:              | <input type="text" value="AES 128"/>           |
| Action:                            | <input type="text" value="Encrypt"/>           |
| Action on failure:                 | <input type="text" value="Drop and send DSN"/> |

Create

Cancel

## 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**.

## How to integrate FortiMail into Microsoft 365

This recipe describes how to integrate FortiMail unit with Microsoft 365 to protect your incoming and outgoing email. For information about FortiMail Cloud integration, see [FortiMail Cloud Integration With Microsoft 365 Deployment Guide](#).

### Configuring domain and DNS settings in Office 365

Use the following steps to configure your new domain within Office 365.



In the event the following steps become out-dated, please refer to the following links from Microsoft online help:

- [Add a domain to Microsoft 365](#)
- [Add another domain](#)

In the Microsoft 365 admin center, select **Setup**.

1. Under **Get your custom domain set up**, select **View**.
2. Select **Manage**, and then **Add domain**.
3. Enter the new domain name that you want to add, and select **Next**.

The screenshot shows the 'Add a domain' interface in the Microsoft 365 admin center. On the left, there's a sidebar with a '+ Add domain' button and a list of domains including 'contosoco.com (Default)' and 'rycontoso.onmicrosoft.com'. The main area is titled 'Add a domain' and contains a form. The form has a text input field with the value 'contosocos.com' and a preview text: 'Your users' email addresses will look like this: username@contosocos.com'. At the bottom of the form are two buttons: 'Next' and 'Close'.

4. Sign in to your domain registrar (for example, GoDaddy), and select Next.

5. If prompted, sign in to your registrar, and select **Authorize**.
6. Select **Add DNS records for me**, and select **Next**.
7. Choose the services for your new domain and clear the check boxes for any services that will be handled by a different domain.  
For example, if you only want to use the new domain for email, select **Exchange**, and clear the check boxes for **Skype for Business** and **Mobile Device Management for Office 365**.
8. Follow the remaining prompts to finish adding your new domain.
9. Next, go to your DNS server.
10. Change the MX record from Office 365 to your FortiMail unit.

**Manage your DNS** for **tryptichconsulting.com**

**Basic DNS** **Advanced DNS**

**Advanced DNS is recommended for advanced users only, and allows full customisation of your DNS settings.** Using this form will disable the basic DNS view.

**Warning:** If you have an @ record set to a CNAME, all other @ records (including MX) will be ignored and set to the same domain to which it points.

| DNS ENTRY | TYPE    | PRIORITY | TTL | DESTINATION/TARGET      |
|-----------|---------|----------|-----|-------------------------|
| *         | A       |          |     | 81.21.76.62             |
| @         | A       |          |     | 81.21.76.62             |
| @         | MX      | 10       |     | mail.tryptichconsult... |
| mail      | A       |          |     | 86.152.19.82            |
| @         | TXT/SPF |          |     | MS=ms86440163           |

Hostname:  (eg: @tryptichconsulting.com)

Type: **TXT/SPF**

Destination TXT/SPF:  (eg: Some free text)

**Add**

**Delete all records**

## Configuring FortiMail to accept Office 365

Next, configure your FortiMail unit to accept mail from your domain and then forward the mail to Office 365.

1. In FortiMail, go to **Domain & User > Domain > Domain**.
2. Select **New**, or double-click a domain to edit an existing domain.
3. Enter the **Domain name**, and enter the **SMTP server**.

4. When finished, select **Create**, or **OK**.

FortiMail

Domain name:

Is subdomain

☐

Main domain:

Relay type:

Host

SMTP server:

Port:

25

[Test...]

☐ Use SMTPS

Fallback SMTP server:

Port:

25

[Test...]

☐ Use SMTPS

☐ Relay Authentication

☐ Recipient Address Verification

☐ Automatic Removal of Invalid Quarantine Accounts

☐ LDAP Options

☐ Advanced Setting

Create

Cancel

## Configuring Office 365 to accept FortiMail

Next, configure Office 365 to accept incoming mail, once it's been checked, from your FortiMail unit.

1. In Office 365, go to the [Exchange administrator center](#).
2. From the drop-down menu, select **Create a new rule**.

Exchange admin center

Home

Recipients

Mail flow

Message trace

Rules

Remote domains

Accepted domains

Connectors

Alerts

Alert policies

Roles

Migration

Reports

Insights

Organization

Public folders

Settings

# Rules

If you're using Google Chrome incognito and this page isn't working, enable third-party cookies. [Learn more about managing Google Chrome cookies.](#)

Rules

Create a new rule...

Apply Office 365 Message Encryption and rights protection to messages...

Apply custom branding to OME messages...

Apply disclaimers...

Bypass spam filtering...

Filter messages by size...

Generate an incident report when sensitive information is detected...

Modify messages...

Restrict managers and their direct reports...

Restrict messages by sender or recipient...

Send messages to a moderator...

Send messages and save a copy for review...

|  | PRIORITY |
|--|----------|
|  | 0        |
|  | 1        |

0 selected of 2 total

3. Enter a **Name** for the new rule, and select **More options**.

new rule - Google Chrome

outlook.office365.com/ecp/RulesEditor/NewTransportRule.aspx?ActivityCorrelationID=a097b55f-7c1d-f...

new rule

Name:  
Accept on from FML

\*Apply this rule if...  
Select one

\*Do the following...  
Select one

Properties of this rule:

☒ Audit this rule with severity level:  
Not specified

Choose a mode for this rule:

☒ Enforce  
☐ Test with Policy Tips  
☐ Test without Policy Tips

More options...

Rights Management Services (RMS) is a premium feature that requires an Enterprise Client Access License (CAL) or a RMS

Save Cancel

4. Configure the rule's **condition** and **action**, as required.

Rule - Google Chrome

outlook.office365.com/ecp/RulesEditor/EditTransportRule.aspx?ActivityCorrelationID=f0562c17-5360-b9b4-8b3a-00...

Accept on from FML

Name:  
Accept on from FML

\*Apply this rule if...  
The sender is located... [Outside the organization](#)  
add condition

\*Do the following...  
Delete the message without notifying anyone  
add action

Except if...  
✕ Sender's IP address is in the range... ['82.98.199.46'](#)  
add exception

Properties of this rule:  
Priority:  
0

☒ Audit this rule with severity level:  
Not specified

Save Cancel

5. Enter the IP address of the FortiMail unit as the rule's **exception**, and select **OK**.

new rule - Google Chrome

outlook.office365.com/ecp/RulesEditor/NewTransportRule.aspx?ActivityCorrelationID=a097b55f-7c1d-f09b-f88c-8ce...

new rule

add condition

\*Do the following...

Delete the message without n

add action

Except if...

✕ Sender's IP address is in the r

add exception

Properties of this rule:

☒ Audit this rule with severity

Not specified ▼

Choose a mode for this rule:

☒ Enforce

☐ Test with Policy Tips

☐ Test without Policy Tips

specify IP address ranges

Enter an IPv4 or IPv6 address, or range +

OK Cancel

Save Cancel



Additionally, you may add another exception that will match if the Received header includes your FortiMail hostname (found in FortiMail under **System > Mail Setting > Mail Server Setting**).

This exception means that if the email has already been scanned by FortiMail, it will not then be sent back again to FortiMail.

6. Configure another new rule to drop all incoming mail, **unless** it comes from FortiMail servers.
7. Once the rule is created, enable it from the **ON** column of the **Rules** section of the Exchange administrator center.

Exchange admin center

Rules

ⓘ If you're using Google Chrome incognito and this page isn't working, enable third-party cookies. [Learn more about managing Google Chrome cookies.](#)

Rules

⊕ ✎ 🗑️ ⬆️ ⬇️ ⬇️ 🔍 ↺

| ON                                  | RULE               | PRIORITY |
|-------------------------------------|--------------------|----------|
| <input checked="" type="checkbox"/> | Accept on from FML | 0        |

---

## Configuring outbound settings in FortiMail

Now that inbound settings are configured in both Office 365 and FortiMail, you must next configure outbound settings in FortiMail.

1. In FortiMail, go to **Dashboard > Console** to open the CLI console.
2. Enter the following commands, for each Office 365 server IP address, to add Office 365 as a trusted relay to FortiMail:

```
config policy access-control receive
  edit 1
    set sender-ip-mask 23.103.132.0/22
    set action relay
  next
  edit 2
    set sender-ip-mask 23.103.144.0/22
    set action relay
  next
  edit 3
    set sender-ip-mask 23.103.191.0/24
    set action relay
  next
  edit 4
    etc...
```

## Configuring outbound settings in Office 365

Finally, configure an Office 365 connector to relay outgoing mail to FortiMail.

1. From the Exchange administrator center, go to **Mail Flow > Connectors > Add a connector**.
2. Set **Connection from** to **Office 365**, and set **Connection to** to **Partner organization**, and select **Next**.

**Add a connector**×

New connector

Name

Use of connector

Routing

Security restrictions

Validation email

Review connector

## New connector

Specify your mail flow scenario, and we'll let you know if you need to set up a connector.

**Connection from**

☒ Office 365

☐ Your organization's email server

☐ Partner organization

**Connection to**

☐ Your organization's email server

☒ Partner organization

**Next**

3. Enter a **Name** and **Description** for the connector, and select **Next**.

Add a connector
×

✓
New connector

●
Name

○
Use of connector

○
Routing

○
Security restrictions

○
Validation email

○
Review connector

## Connector name

This connector lets Office 365 deliver messages to your organization's email server.

**Name \***

**Description**

**What do you want to do after connector is saved?**

☒ Turn it on

☒ Retain internal Exchange email headers (recommended)

Back
Next

4. Enable **Only when I have a transparent rule set up that redirects messages to this connector**, and select **Next**.
5. Configure the IP address or FQDN of the FortiMail, and select **Next**.
6. Enable **Any digital certificates, including self-signed certificates**, and select **Next**.
7. Review the new connector settings and select **Next**.
8. Select **Validate**. Office 365 will perform the steps necessary for successful validation.
9. When it's finished, select **Close**. The **Status** section will show as **Succeeded**. Select **Save**.

Your incoming and outgoing messages will now be protected by FortiMail.

It's advised to take the time to apply FortiMail AntiVirus and AntiSpam profiles as appropriate.



If you choose, you may safely disable Office 365 Antispam services, if you regard it as no longer required.

## 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.

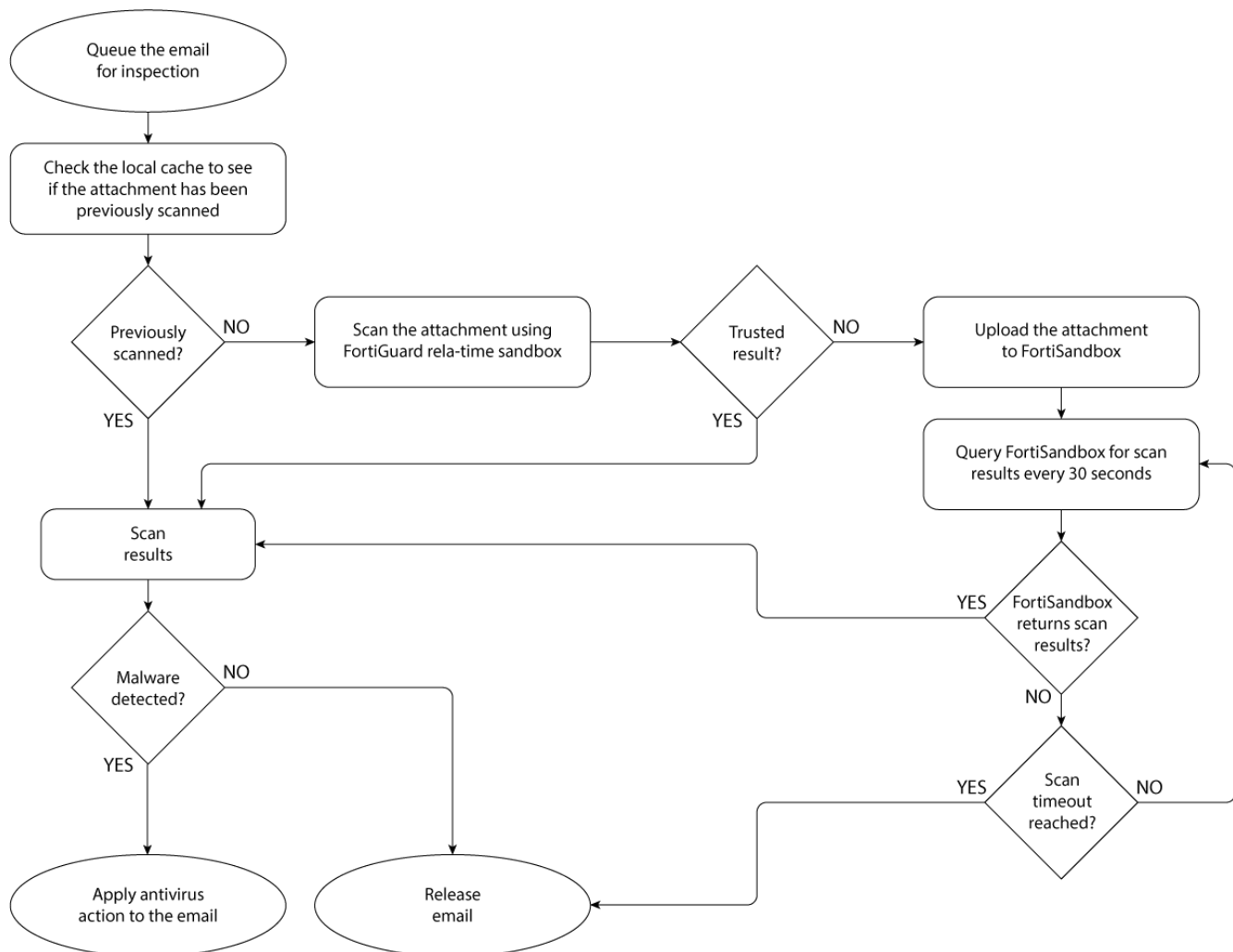
## Integrating FortiSandbox with FortiMail

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.



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, xlsxm, xltm, xlsb, xlsm
- 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**

FortiSandbox Inspection ☐ Statistics...

FortiSandbox type: Appliance Cloud **Enhanced Cloud**

Server name/IP:

Notification email:

Statistics interval:  (minutes)

Scan timeout:  (minutes)

Scan result expires in:  (minutes)

☒ **File Scan Setting**

File types: ☒ Windows executable ☒ Microsoft Office document  
☒ PDF ☒ Adobe flash  
☒ JavaScript ☒ Jar  
☒ HTML ☒ Archive

File patterns:

File size: ☐ Maximum file size to upload  (KB)

☒ **URL Scan Setting**

Email selection: **All email** Suspicious email

URL selection: all

Upload URL on rating error ☐

Number of URLs per email:

---

## 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



+ New...

Edit...

### Profiles

AntiSpam:

--None--



+ New...

Edit...

AntiVirus:

FSA-analysis



+ New...

Edit...

Content:

--None--



+ New...

Edit...

Resource:

Res\_Default



+ New...

Edit...

### Authentication and Access

### Advanced Settings

Create

Cancel

## 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**.

## Securing outbound email from Google Workspace

In this recipe, you will configure Google Workspace (formerly G Suite) for secure outbound email through FortiMail or FortiMail Cloud.

For this configuration, FortiMail/FortiMail Cloud operates in Gateway mode to perform as the secure outbound email gateway for messages originating from the Google Workspace email server.

Once you have linked your Google Workspace account to FortiMail, you will then configure access control and recipient outbound policies on FortiMail for outbound email.



At the time of writing, some topics reference Google's help section titled [Set up an outbound mail gateway](#). It is recommended that you check the Google help page for any subsequent updates.



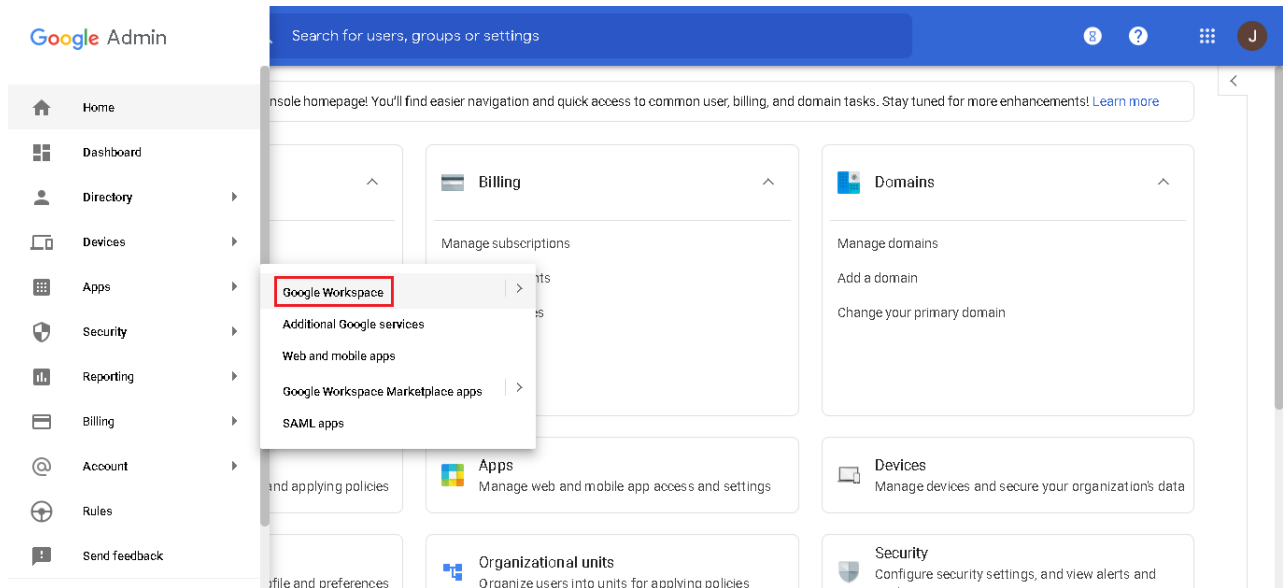
FortiMail can scan internal to external email, however there is currently no support for internal to internal scanning.

---

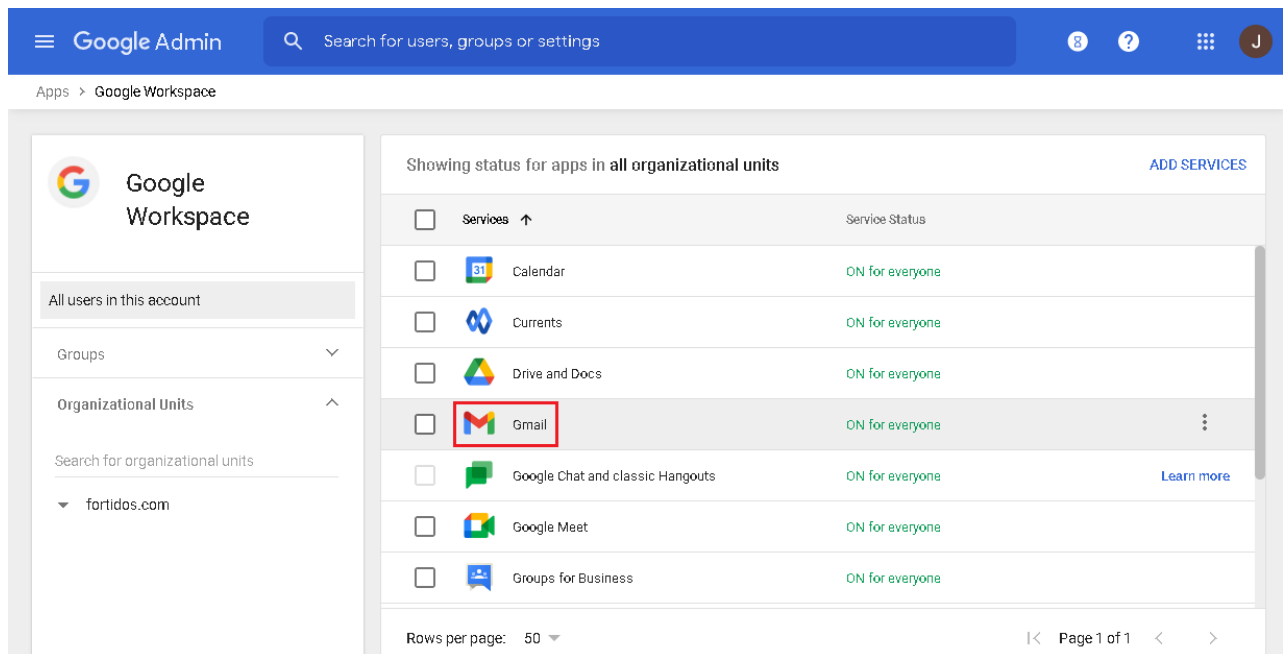
## Add FortiMail as mail route host in Google Workspace

This topic describes how to add FortiMail/FortiMail Cloud as the mail route host.

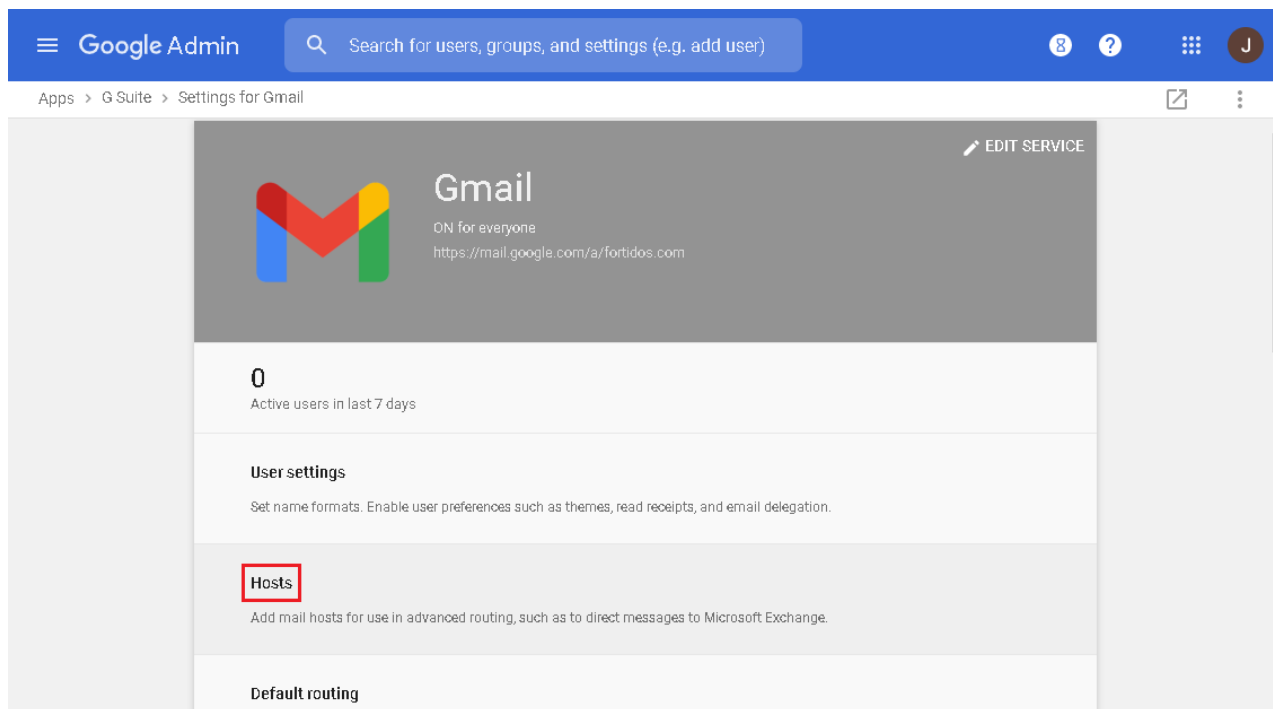
1. Log in to [Google Workspace](#) using your administrative credentials.
2. From the *Admin Console* dashboard, click the expandable *Main menu* and click *Apps > Google Workspace*.



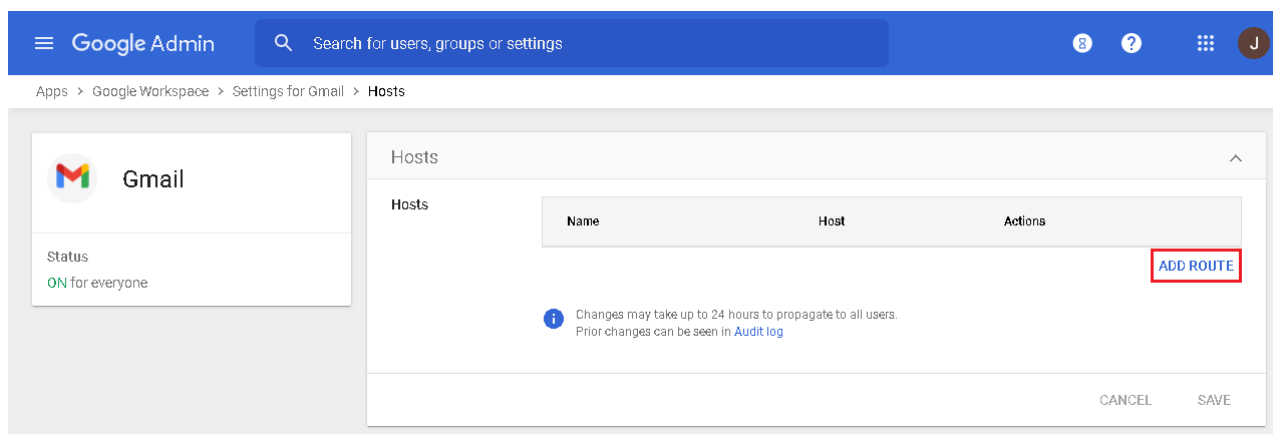
3. From the list of services available, click *Gmail*.



4. From the *Settings for Gmail* page, click *Hosts*.



5. Click *Add Route*.



6. Enter a *Name* for the mail route host.

7. Under *Specify email server*, enter the host name or IP address of FortiMail/FortiMail Cloud.

## Edit mail route

Name

[Learn more](#)

**fmlcloud**

This field is required.

1. Specify email server

Only ports numbered 25, 587, and 1024 through 65535 are allowed.

Single host ▼

:

8. Under *Options*, for maximum security, confirm that TLS and CA signed certificate requirements are enabled. Click *Test TLS connection* to verify a successful TLS connection between Google Workspace and the FortiMail unit.

## Edit mail route

### 2. Options

- ☐ Perform MX lookup on host
- ☒ Require mail to be transmitted via a secure (TLS) connection (Recommended)
- ☒ Require CA signed certificate (Recommended)
  - ☒ Validate certificate hostname (Recommended)

[Test TLS connection](#)

TLS connection validated on June 17, 2021  
11:16 AM

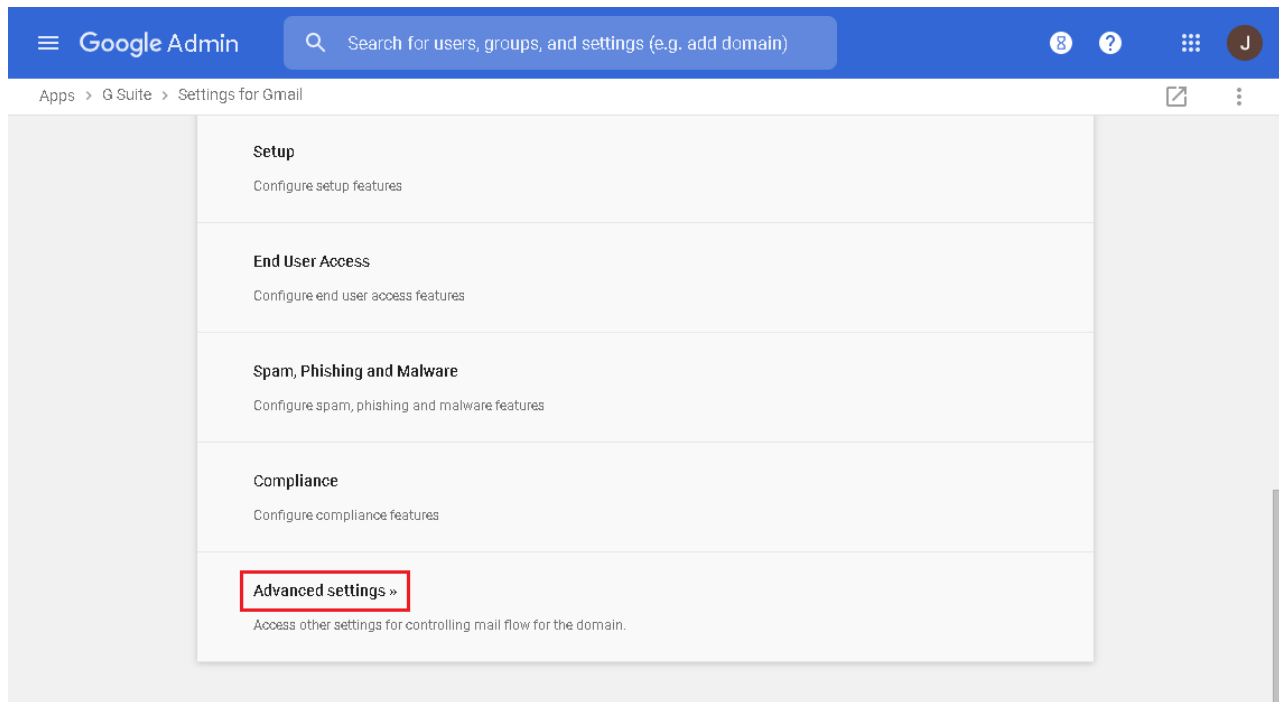
CANCEL [SAVE](#)

9. Click Save.

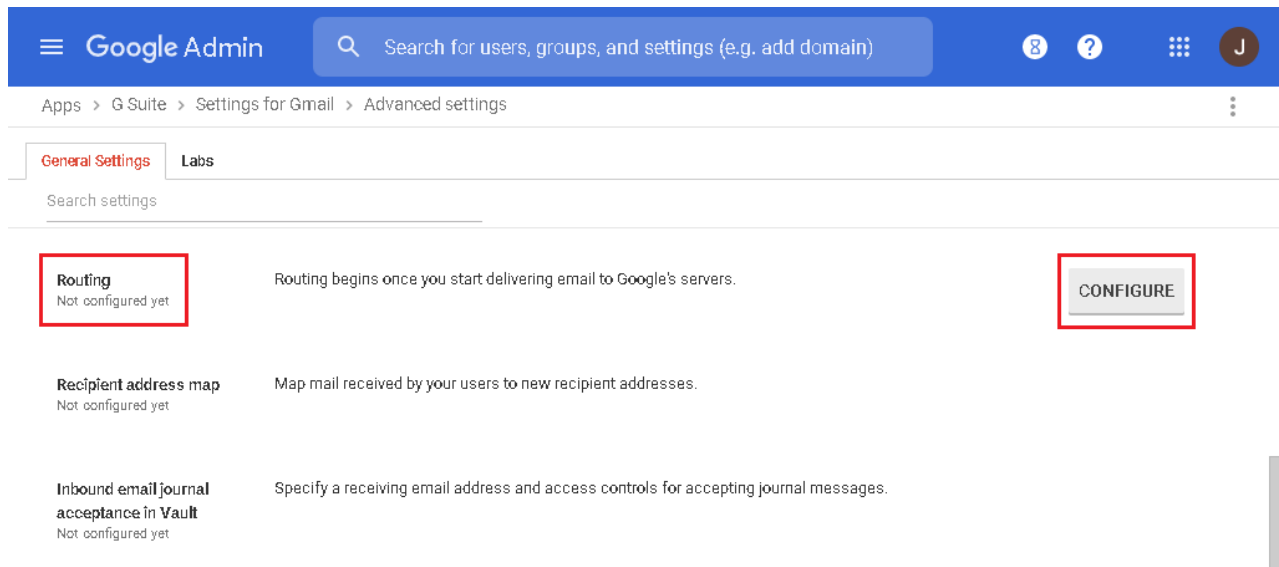
## Route all outbound mail from Google Workspace through FortiMail

This topic describes how to route all messages from your Google Workspace domain through FortiMail performing as the gateway server.

1. Navigate back to the *Settings for Gmail* screen and click *Advanced settings*.



2. From the *General Settings* tab, hover over the *Routing* section and click *Configure*.



3. Enter a mandatory short description for the new routing setting.
4. Under *Messages to affect*, enable *Outbound*.
5. Optionally, under *Envelope filter*, enable *Only affect specific envelope recipients*.  
From the drop-down menu, select *Pattern match*, and enter a suitable *Regex* pattern (in this example, `.*@live\.cn`).

Add setting

Routing

fmcloud

1. Messages to affect

☐ Inbound

☒ Outbound

☐ Internal - sending

☐ Internal - receiving

2. Envelope filter

☐ Only affect specific envelope senders

☒ Only affect specific envelope recipients

Pattern match

Regexp [Learn more](#)

.\*@live\.cn

Test expression

6. Further down, under *Route*, enable *Change route*, and select the mail route host you created in the previous topic (in this example, fmcloud).
7. Click *Add Setting*.

Add setting

3. For the above types of messages, do the following

Modify message

Headers

☐ Add X-Gm-Original-To header

☐ Add X-Gm-Spam and X-Gm-Phishy headers

☐ Add custom headers

Subject

☐ Prepend custom subject

Route

☒ Change route

☐ Also reroute spam

☐ Suppress bounces from this recipient

fmlcloud

CANCEL

ADD SETTING

## Configure access control rule and recipient policy on FortiMail

This topic shows how to configure an access control rule on FortiMail to accept and relay the email from Google Workspace and how to configure an recipient policy to scan the email.

### To add an ACL rule for Google Workspace

1. On the FortiMail admin GUI, go to *Policy > Access Control > Receiving*.
2. Click *New* to create a new access control rule.
3. Configure the following:
  - Enabled: Select whether or not the access control rule is currently in effect.
  - Sender: Specify the sender patterns appropriate to cover the email senders from Google Workspace.
  - Recipient: Specify the recipient patterns appropriate to cover the email senders from Google Workspace.
  - Source: Specify the email server using the appropriate format.
  - Reverse DNS pattern: Enter a pattern to compare to the result of a reverse DNS look-up of the IP address of the SMTP client delivering the email message.

- 
- Authentication status: Select whether or not to match this access control rule based on client authentication.
    - Any: Match or do not match this access control rule regardless of whether the client has authenticated with the FortiMail unit.
    - Authenticated: Match this access control rule only for clients that have authenticated with the FortiMail unit.
    - Not Authenticated: Match this access control rule only for clients that have **not** authenticated with the FortiMail unit.
  - TLS profile: Select a TLS profile to allow or reject the connection based on whether the communication session attributes match the settings in the TLS profile.
  - Action: Select the Relay action.
  - Comments: Enter a comment if necessary. The comment will appear as a mouse-over tool-tip in the ID column of the rule list.

### **To add a scan policy**

1. On the FortiMail admin GUI, go to Policy > Recipient Policy > Outbound.
2. Click *New* to create a new scan policy for outbound email from Google Workspace.
3. Make sure that all the domains on Google Workspace are covered. For details about adding a recipient based outbound policy, see the FortiMail Administration Guide.

## 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 shows you how to enable SMTP authentication and check the SMTP authentication score and record. This recipe is undertaken solely in the CLI.

Use the following CLI commands to enable SMTP authentication. 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
```

To display automatically added exempt IP addresses, enter the following CLI command:

```
diagnose system authserver display auto-exempt
```

To delete the IP address, enter the following CLI command:

```
diagnose system authserver delete auto-exempt <ip_address>
```

## 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.

The screenshot shows the FortiMail VM02 Status page. The left sidebar contains a navigation menu with items: Dashboard, FortiView, Monitor, System, Domain & User, Policy, Profile, Security, Encryption, Data Loss Prevention, Email Archiving, and Log & Report. The main content area is titled 'Status' and 'Console'. It features two expandable widgets. The 'System Information' widget displays the following details: Serial number (FEVM020000), 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), and Email throughput (0 messages per minute (last 60 minutes) Spam: 0, Not Spam: 0 messages per minute). The 'License Information' widget shows AntiVirus as Licensed (Expiry date: 2021-03-28) with a green checkmark, and AV definition as Version 79.00549 (Last updated: 2020-08-11 10:15:00) [Update...]. At the bottom, a file download bar shows 'config\_v64b0384\_2....cfg'.

## 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.

## Upload

5%

FML\_VM-64-v64-build0414-FORTINET.out

[99.7 M]

Cancel

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.

The screenshot shows the FortiMail VM02 web interface. The top navigation bar is green with the FortiMail logo and the text 'FortiMail VM02 FortiMail'. Below this is a sidebar menu with various icons and labels: Dashboard, FortiView, Monitor, System, Domain & User, Policy, Profile, Security, Encryption, Data Loss Prevention, Email Archiving, and Log & Report. The main content area has two tabs: 'Status' (selected) and 'Console'. The 'Status' tab displays a 'System Information' window with the following details:

| System Information     |                                                                                 |
|------------------------|---------------------------------------------------------------------------------|
| 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 <a href="#">[Update...]</a>                     |
| System configuration:  | <a href="#">[Backup...]</a> <a href="#">[Restore...]</a>                        |
| Operation mode:        | Gateway                                                                         |
| Current administrator: | admin (1 in total) <a href="#">[Details...]</a>                                 |
| 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).

FortiMail VM04

FortiMail

?

admin

Dashboard

FortiView

Monitor

Log

Quarantine

Mail Queue

Greylist

Reputation

Archive

Report

Centralized Monitor

System

History

System Event

Mail Event

AntiVirus

AntiSpam

Encryption

List

Level: Information

Sub type: All

View

Search

Export

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

Configure View

1

/ 21

Records per page: 100

Go to line:

Total: 2090

| # | Date       | Time         | Subtype | Message                                                                             | Level       | Log ID     |
|---|------------|--------------|---------|-------------------------------------------------------------------------------------|-------------|------------|
| 1 | 2020-08-11 | 11:08:15.834 | ha      | remote-hasynod (172.20.142.228): hasynod: starting                                  | notice      | 0703002060 |
| 2 | 2020-08-11 | 11:06:34.860 | ha      | remote-hasynod (172.20.142.228): hasynod: 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-hasynod (172.20.142.228): hasynod: starting                                  | notice      | 0703002059 |
| 6 | 2020-08-11 | 10:03:04.426 | ha      | remote-hasynod (172.20.142.228): hasynod: shutting down                             | notice      | 0703002060 |
| 7 | 2020-08-11 | 10:02:42.731 | ha      | remote-hasynod (172.20.142.228): hasynod: config_receive: retrieving initial config | notice      | 0703002055 |

- 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.

[www.fortinet.com](http://www.fortinet.com)



Copyright© 2024 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.