Encrypting Confidential Emails in FortiMail

You want to send an email containing sensitive information, but you're afraid 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:

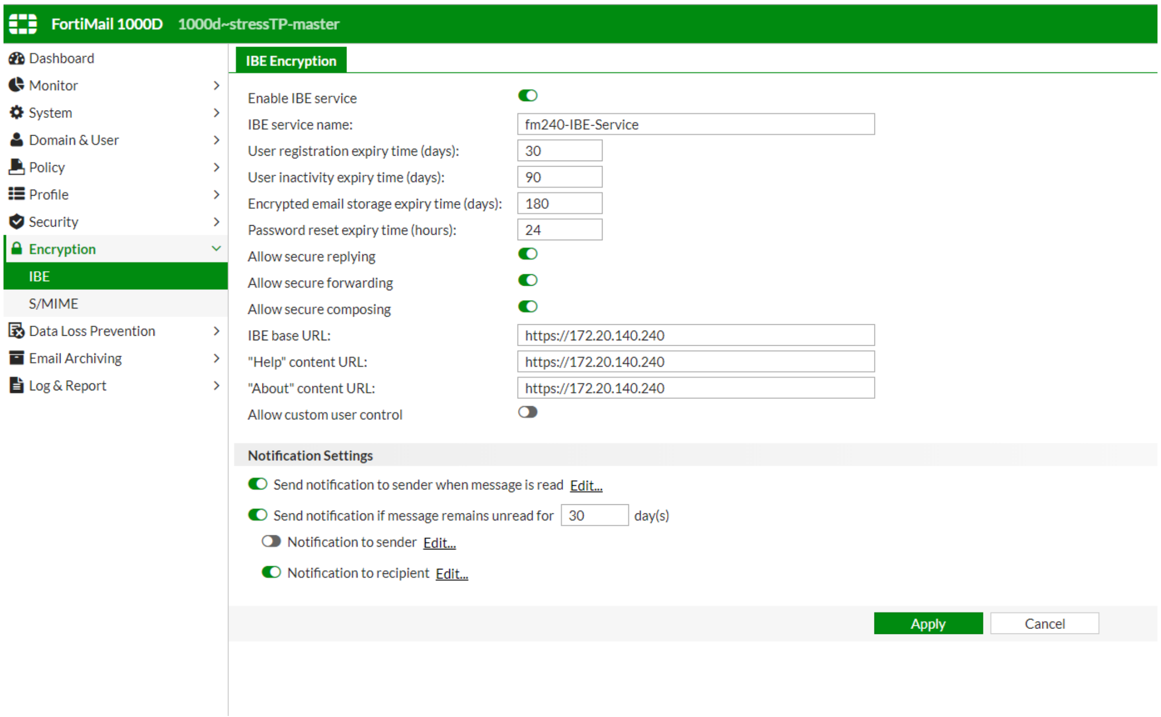
- **Content-based encryption:** The FortiMail unit can find key words in an email's subject header or message body to determine if a message should be encrypted. For example, if you add "Confidential" in your subject header, FortiMail will encrypt the email message.
- **Rule-based encryption:** The FortiMail 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

First we'll need to enable the IBE service

1. Navigate to **Encryption > IBE > IBE Encryption.**



Enable IBE service ●
IBE service name: fm240-IBE-Service
User registration expiry time (days): 30
User inactivity expiry time (days): 90
Encrypted email storage expiry time (days): 180
Password reset expiry time (hours): 24
Allow secure replying ●
Allow secure forwarding ●
Allow secure composing ●
IBE base URL: https://172.20.140.240
"Help" content URL: https://172.20.140.240
"About" content URL: https://172.20.140.240
Allow custom user control ○

Notification Settings

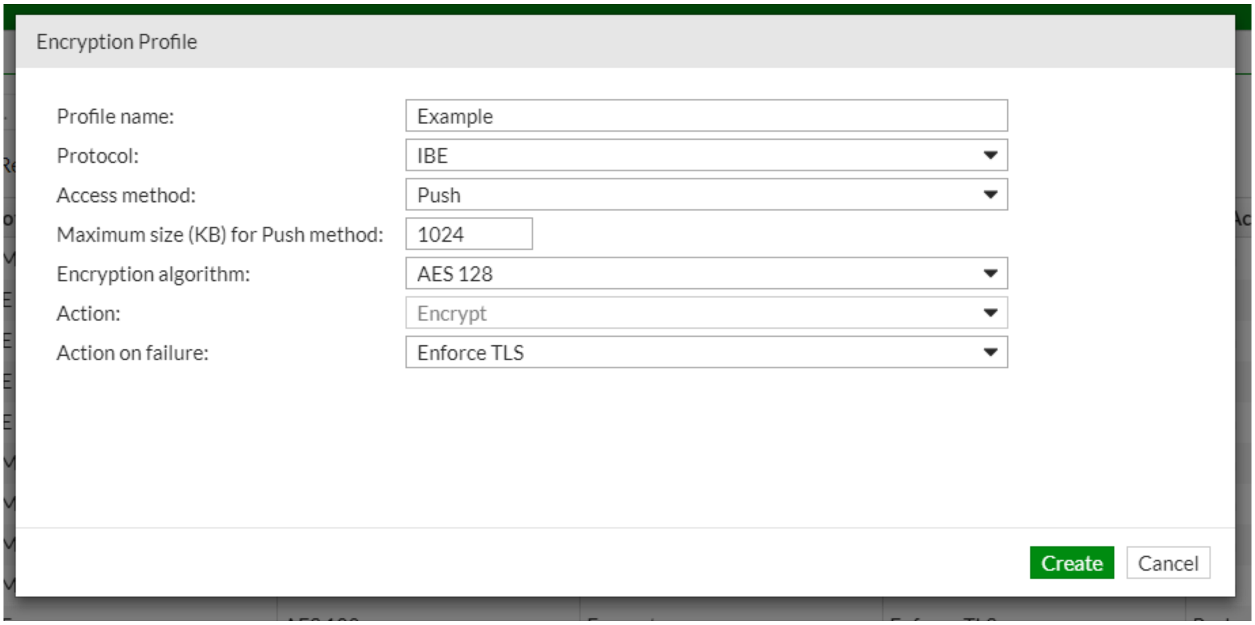
● Send notification to sender when message is read Edit...
● Send notification if message remains unread for 30 day(s)
○ Notification to sender Edit...
● Notification to recipient Edit...

2. Enable IBE service
3. Configure the rest of the appropriate settings.
4. Select **Apply.**

Configuring the Encryption Profile

Now we'll need to configure the encryption profile

1. Navigate to **Profile > Security > Encryption.**
2. Select **New.**



Encryption Profile

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

3. Enter a descriptive name for the encryption profile in the **Profile name** text field.
4. Select IBE from the **Protocol** dropdown menu.

Note: For more information on additional settings in the Encryption Profile, see the FortiMail Administrator guide.

5. Select **Create.**

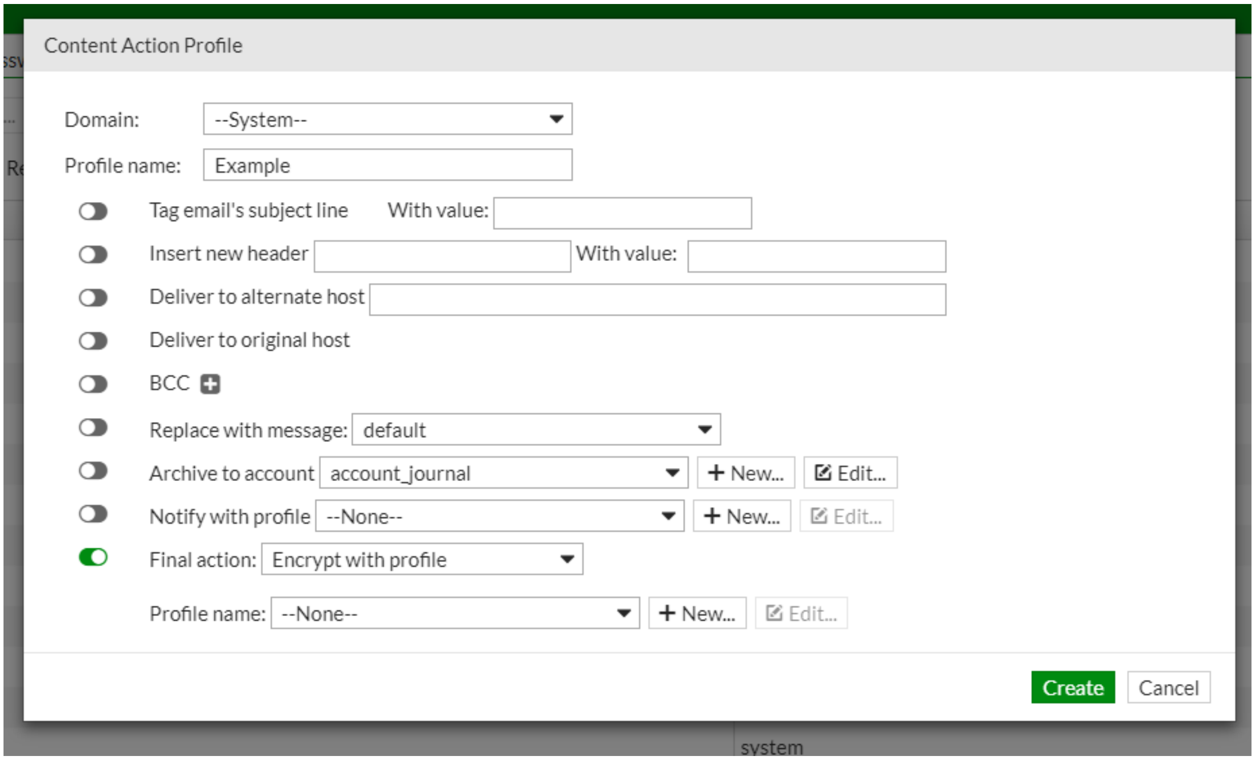
Adding the IBE Encryption Profile

Content action profiles define the action taken by the FortiMail unit when it encounters an email containing a prohibited word or phrase. If you require more detailed information on the Content Action Profile, consult the FortiMail Administrator guide.

To add IBE encryption profile

1. Navigate to **Profile > Content > Action.**

2. Select **New**.



Content Action Profile

Domain: --System--

Profile name: Example

○ Tag email's subject line With value:

○ Insert new header With value:

○ Deliver to alternate host

○ Deliver to original host

○ BCC

○ Replace with message: default

○ Archive to account account_journal

○ Notify with profile --None--

● Final action: Encrypt with profile

Profile name: --None--

3. Enter a descriptive name.
4. Enable Final action and select “encrypt with profile” from the dropdown menu.
5. Select the encryption profile from the Profile name dropdown menu.
6. Configure the rest of the settings as desired.
7. Select **Create.**

Creating a Dictionary Profile

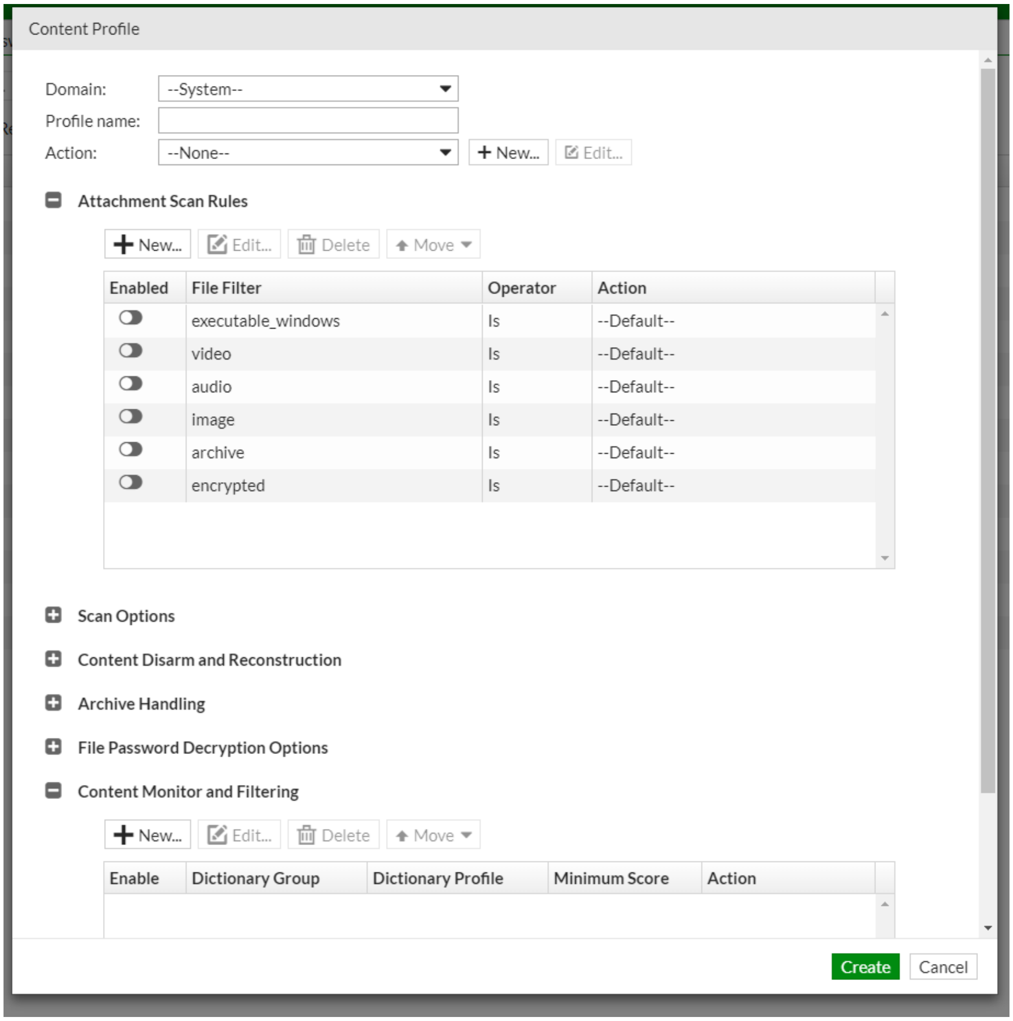
To create a dictionary profile

1. Go to **Profile > Dictionary > Dictionary**.
2. Select **New.**
3. Enter a descriptive name.
4. Select **New** in the Dictionary Entries section.
5. Select **Enable**.
6. Enter “Confidential” in the Pattern textbox.
7. Enable Search header and Search body.
8. Select **Create** and **Create** once more.

Configuring Content Profile

To configure content profiles

1. Go to **Profile > Content > Content**.
2. Select **New.**
3. Expand the **Content Monitor and Filtering** section.



Domain: --System--

Profile name:

Action: --None--

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

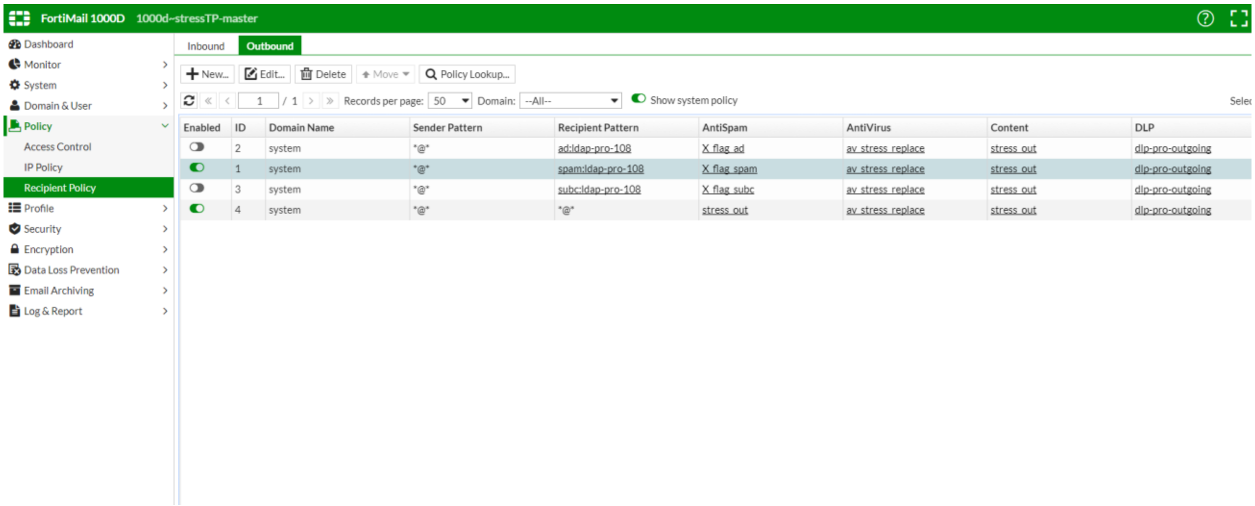
Enable	Dictionary Group	Dictionary Profile	Minimum Score	Action

4. Select **New**.
5. Select **Enable**.
6. Select the recently created dictionary from the **Dictionary** dropdown menu.
7. Select the number of times that an email must match the dictionary profile before it receives the action configured in **Actions**.
8. Select the action you created.
9. Select **Create.**

Configuring Policies

The last step is to configure a policy to use the content profile.

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, you can create a recipient-based policy that uses sender as *@example.com



Records per page: 50 Domain: --All-- Show system policy

Enabled	ID	Domain Name	Sender Pattern	Recipient Pattern	AntiSpam	AntiVirus	Content	DLP
○	2	system	*@*	ad:ldap-pro-108	X flag ad	av stress replace	stress out	dlp-pro-outgoing
●	1	system	*@*	spam:ldap-pro-108	X flag spam	av stress replace	stress out	dlp-pro-outgoing
○	3	system	*@*	subc:ldap-pro-108	X flag subc	av stress replace	stress out	dlp-pro-outgoing
●	4	system	*@*	*@*	stress out	av stress replace	stress out	dlp-pro-outgoing