Preventing Data Loss in FortiMail

One of the biggest fears you'll likely have is the thought of your sensitive data leaving the network. Thankfully, FortiMail has data leak prevention (DLP).

This recipe guides you through the process of enabling DLP, defining sensitive data, and then configuring DLP rules and profiles.

First we will need to enable the DLP feature. Go to the CLI console and enter:

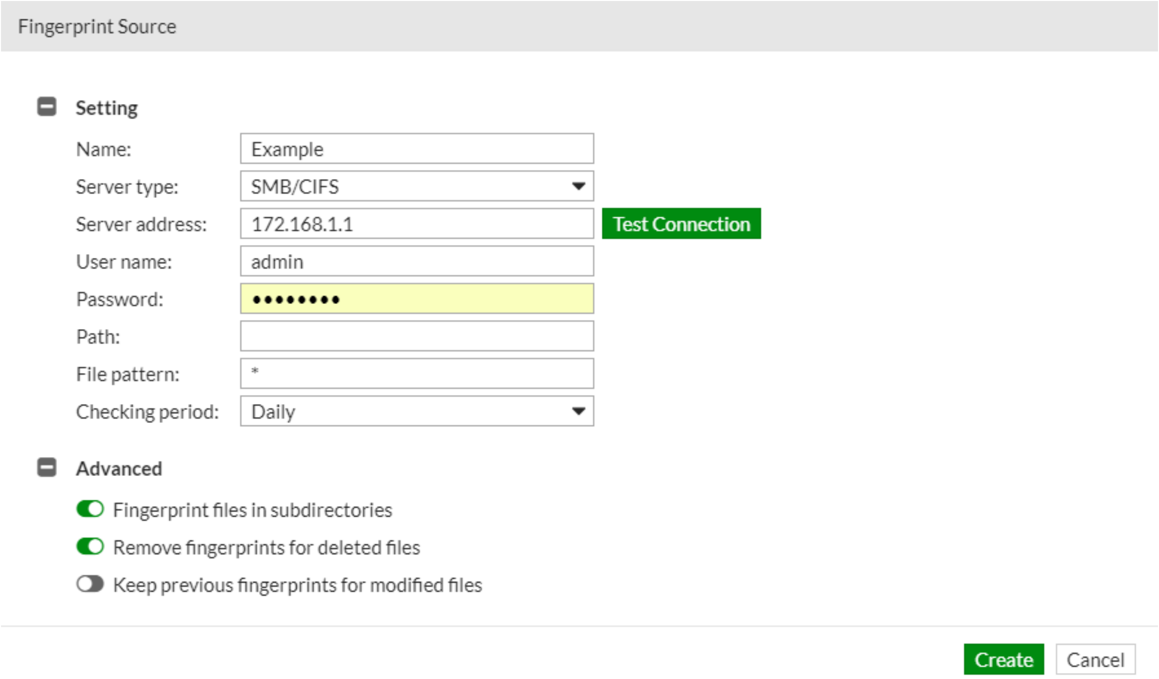
```
config system global
     set data-loss prevention enable
end
```

Defining the Sensitive Data

We will need to configure manual document fingerprints. Document fingerprinting relies on you providing a characteristic of a file that you want to detect. The FortiMail unit generates a checksum fingerprint and stores it. The unit generates a fingerprint for all email attachments and compares them to all the fingerprints stored in the database.

To configure manual document fingerprints:

1. Go to **Data Loss Prevention** > **Sensitive Data** > **Fingerprint.**
2. Select **New**.



Fingerprint Source

Setting

Name:	Example
Server type:	SMB/CIFS
Server address:	172.168.1.1
User name:	admin
Password:	••••••••
Path:	
File pattern:	*
Checking period:	Daily

Advanced

- ● Fingerprint files in subdirectories
- ● Remove fingerprints for deleted files
- ○ Keep previous fingerprints for modified files

3. Enter a name for the fingerprint
4. Select **New** in the File list section and select the file to generate a fingerprint for it.
5. Select **Create**.

You can also configure a fingerprint document source

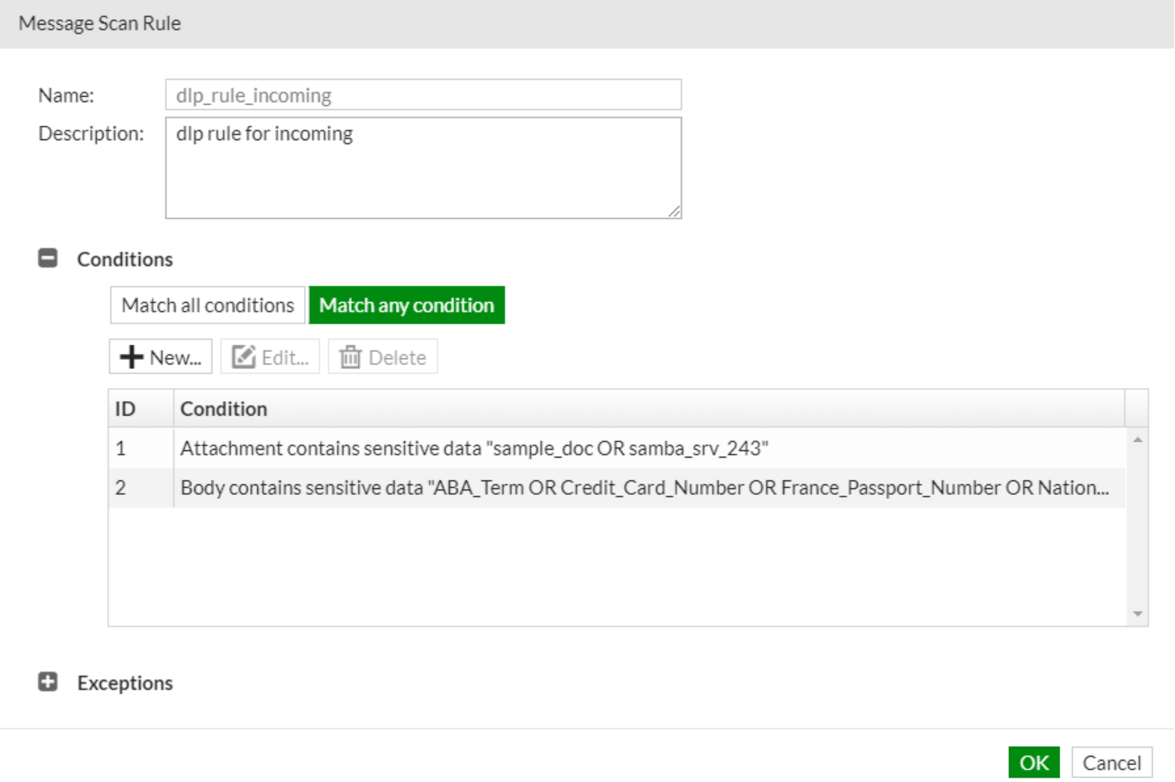
1. Go to **Data Loss Prevention** > **Sensitive Data** > **Fingerprint Source**.
2. Select **New**.
3. Enter a descriptive name and description.
4. Select the server type that is being accessed and enter the IP address of the server.
5. Enter your user name and password.
6. Enter the path to the document folder.
7. Select **Create**.

Configuring DLP Rules

Now we'll configure DLP rules. We'll essentially be telling the unit what to look for when emails. For example, we could scan for sensitive data in email bodies and attachments.

To configure DLP rules

1. Go to **Data Loss Prevention > Rule and Profile > Rule.**



Name: dlp_rule_incoming

Description: dlp rule for incoming

ID	Condition
1	Attachment contains sensitive data "sample_doc OR samba_srv_243"
2	Body contains sensitive data "ABA_Term OR Credit_Card_Number OR France_Passport_Number OR Nation...

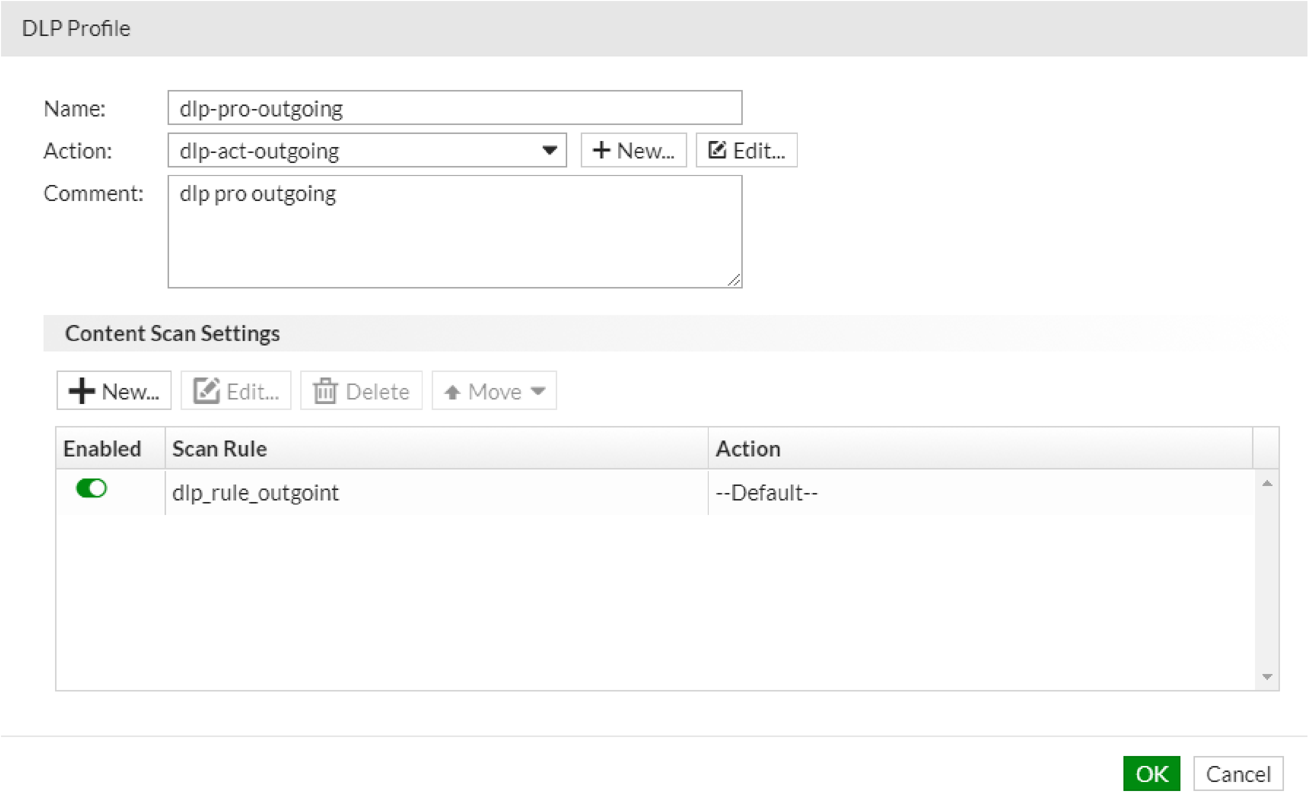
2. Enter a descriptive name for the rule and a description.
3. Select the condition you want to apply to the rule.

Configuring DLP Profiles

After you configure the scan rules/conditions you can add them to DLP profiles. The profile specifies the action to take.

To configure a DLP profile

1. Go to **Data Loss Prevention > Rule and Profile > Profile.**
2. Select **New.**



DLP Profile

Name: dlp-pro-outgoing

Action: dlp-act-outgoing

Comment: dlp pro outgoing

Content Scan Settings

Enabled	Scan Rule	Action
●	dlp_rule_outgoint	--Default--

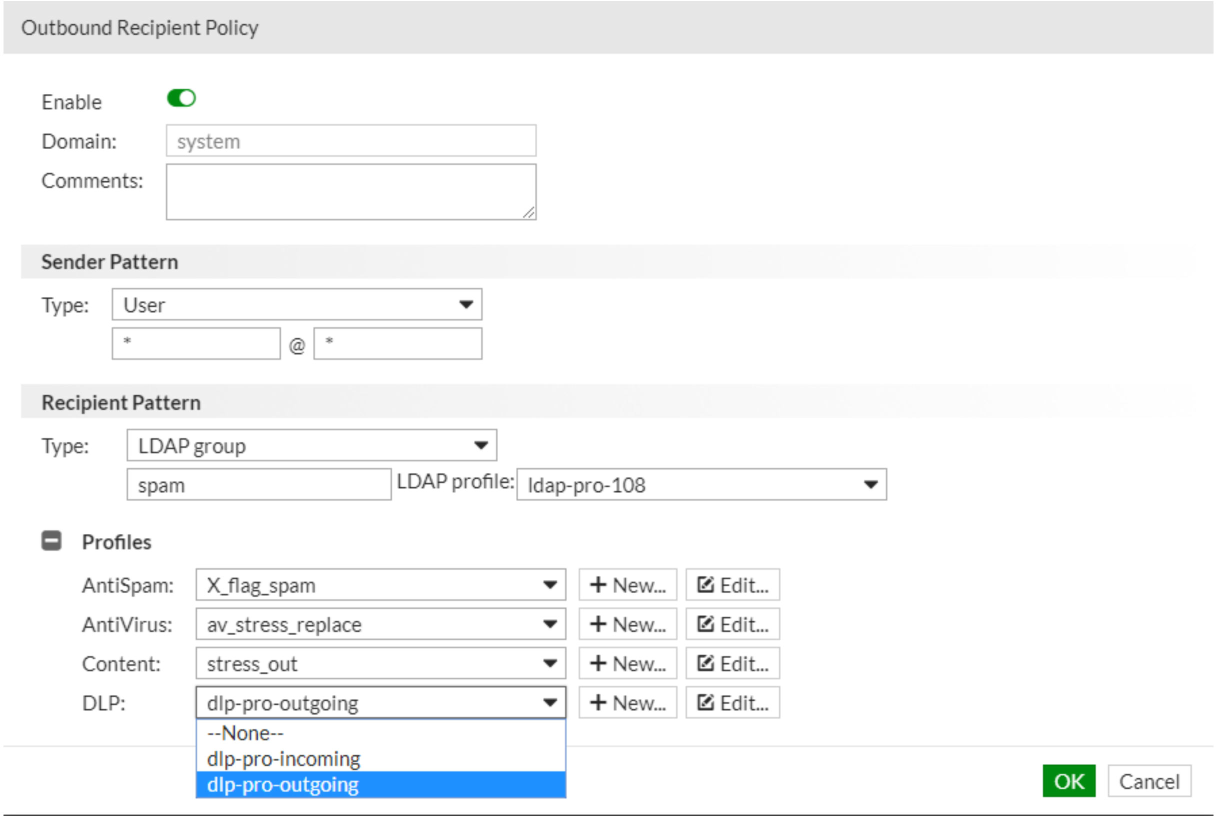
3. Enter a name for the profile.
4. Select the action to use when the specified scan rules match the email.
5. Select **New** in the content scan settings area.
6. Enable the setting.
7. Select your previously created scan rule from the dropdown menu.
8. Select the action profile form the dropdown menu.
9. Select **OK** and then **OK** once more.

Implementing into a Policy

With the profile created, the last thing you`ll need to do is implement the profile into a new or existing policy. The steps are the same, regardless of what type of policy you implement your profile, but for these steps we will use Recipient policies as an example.

To implement your profile

1. Go to **Policy** > **Recipient Policy** > **Outbound**.
2. Select an existing policy and select **Edit**or select **New** to create a new policy.


Outbound Recipient Policy

Enable: ●

Domain: system

Comments:

Sender Pattern

Type: User

* @ *

Recipient Pattern

Type: LDAP group

spam LDAP profile: ldap-pro-108

Profiles

AntiSpam: X_flag_spam

AntiVirus: av_stress_replace

Content: stress_out

DLP: dlp-pro-outgoing

--None--
dlp-pro-incoming
dlp-pro-outgoing

3. Expand the Profiles section.
4. Select your DLP profile in the DLP dropdown menu.
5. Select **OK**.