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

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

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

There are two types of mapping:

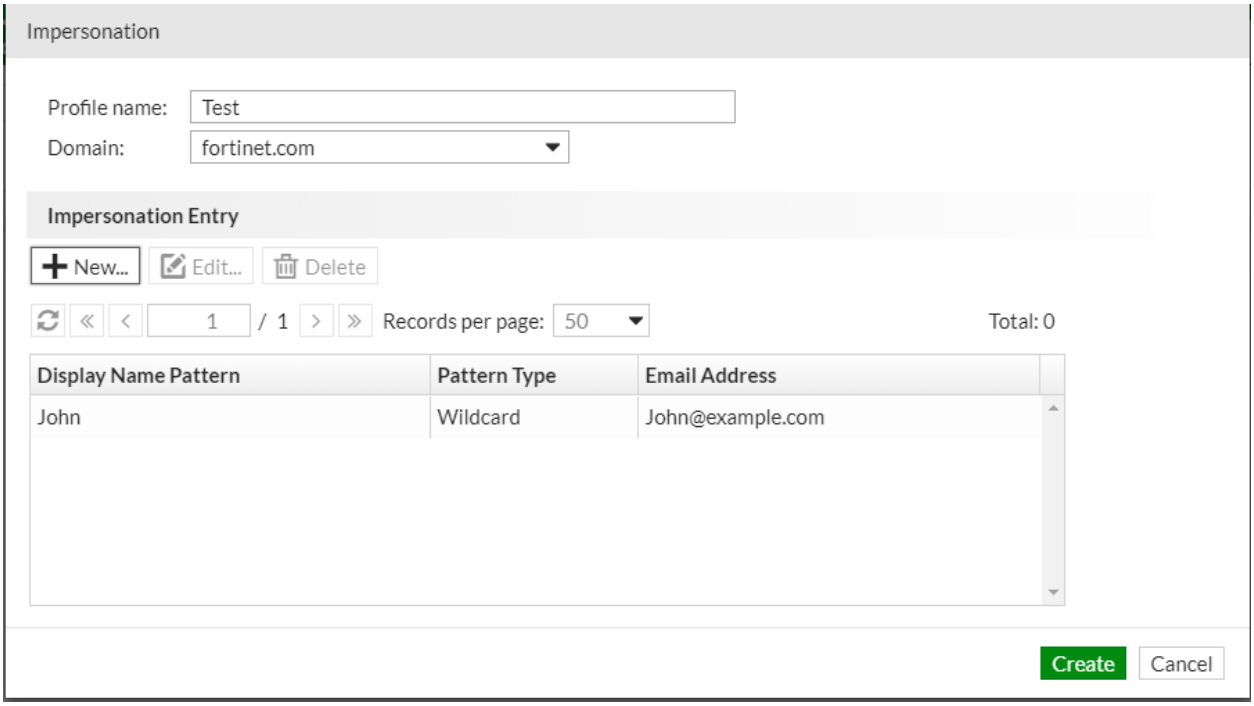
Manual: You manually enter mapping entries and create impersonation analysis profiles as described below and then enable the impersonation profile in an antispam profile. Eventually you apply the antispam profile in the IP-based or recipient-based policies.

Dynamic: FortiMail Mail Statistics Service can automatically learn the mapping. See details below.

Creating an Impersonation Analysis Profile

First you will need to create an impersonation profile and add display names and email addresses to map.

1. Go to **Profile** > **AntiSpam** > **Impersonation**.
2. Select **New** to create a new profile.

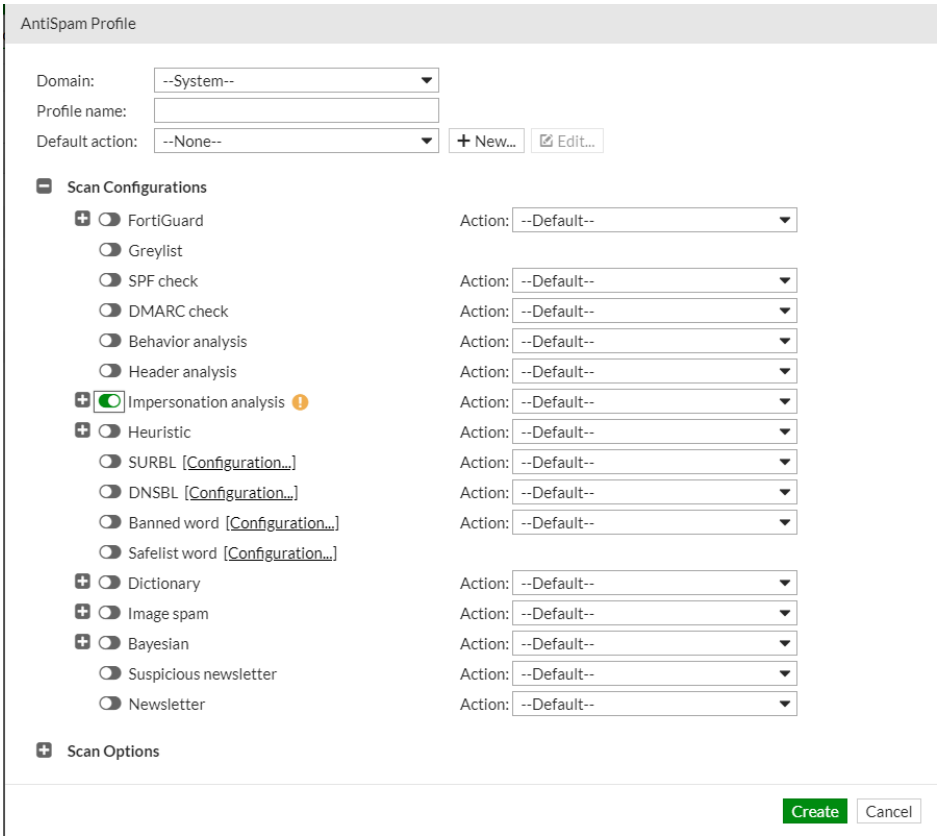


3. Enter an appropriate profile name.
4. Select a domain from the Domain dropdown list.
5. Select **New** in the Impersonation Entry section to add individuals within your business you know to be safe.
6. Enter the display name to be mapped to the email address.
7. Select Wildcard or Regular expression from the Pattern type dropdown list.
8. Enter the email address to be mapped to the display name.
9. Select **Create** and then **Create** once more.

Activating the Impersonation Profile

Now you'll need to enable impersonation analysis in the antispam profile to check for mapping and then select the profile.

1. Go to **Profile** > **AntiSpam** > **AntiSpam**.
2. Select **New** or modify an existing profile.
3. Expand the Scan Configurations section and enable **Impersonation analysis**.



4. Select the desired action you wish the unit to take when it encounters the problem.
5. Select either **Create** or **OK**.
6. When you create an IP policy or recipient policy, choose the antispam profile that contains the impersonation analysis profile.

Viewing 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.

To view the log

1. Go to **Monitor > Log > History**.
2. Select the desired log entry for inspection.
3. Select **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

By default, FortiMail uses manual analysis only.

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

config system global
set mailstat-service enable