Secure Email Threat Defense UI Changes

This document describes changes made to the Secure Email Threat Defense UI in May 2025. These changes are part of Cisco's ongoing efforts to provide a more consistent experience across Cisco Security offerings. Additionally, we have added the ability to set remediation policy by direction. This is described in the section about the new Policy configuration page.

Policy and Configuration Pages

The Policy page has been renamed Configuration and has been split into three separate areas:

- Mail flow configuration
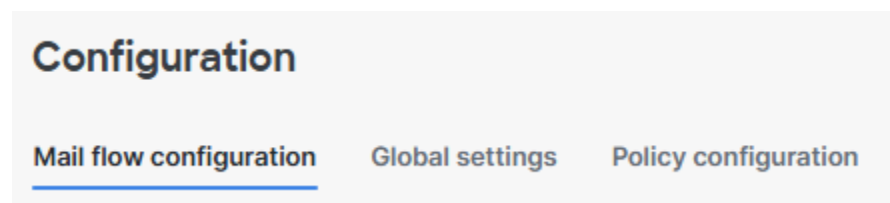- Global settings
- Policy configuration

Figure 1.
New Configuration page areas

In the classic Policy page, you make changes and then must click the **Save and Apply** button. In the new pages, you can edit each panel by clicking the pencil icon in the top right corner. This allows more granular access to your settings. After you click the pencil, you are taken to a dialog for simple settings or to a workflow to change more complicated settings.
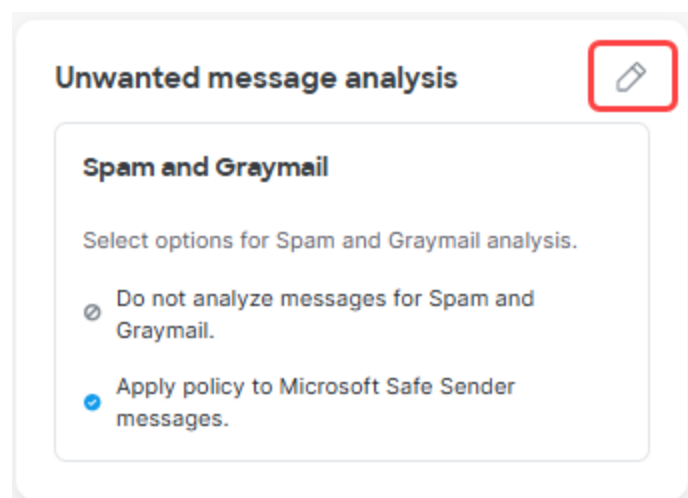

Figure 2.
Use the pencil icon to edit the settings in each panel

Mail flow configuration

The Mail flow configuration page combines the classic Message Source and Visibility panels. This is where you can see and configure your message sources, Microsoft 365 visibility, and manage your domains.
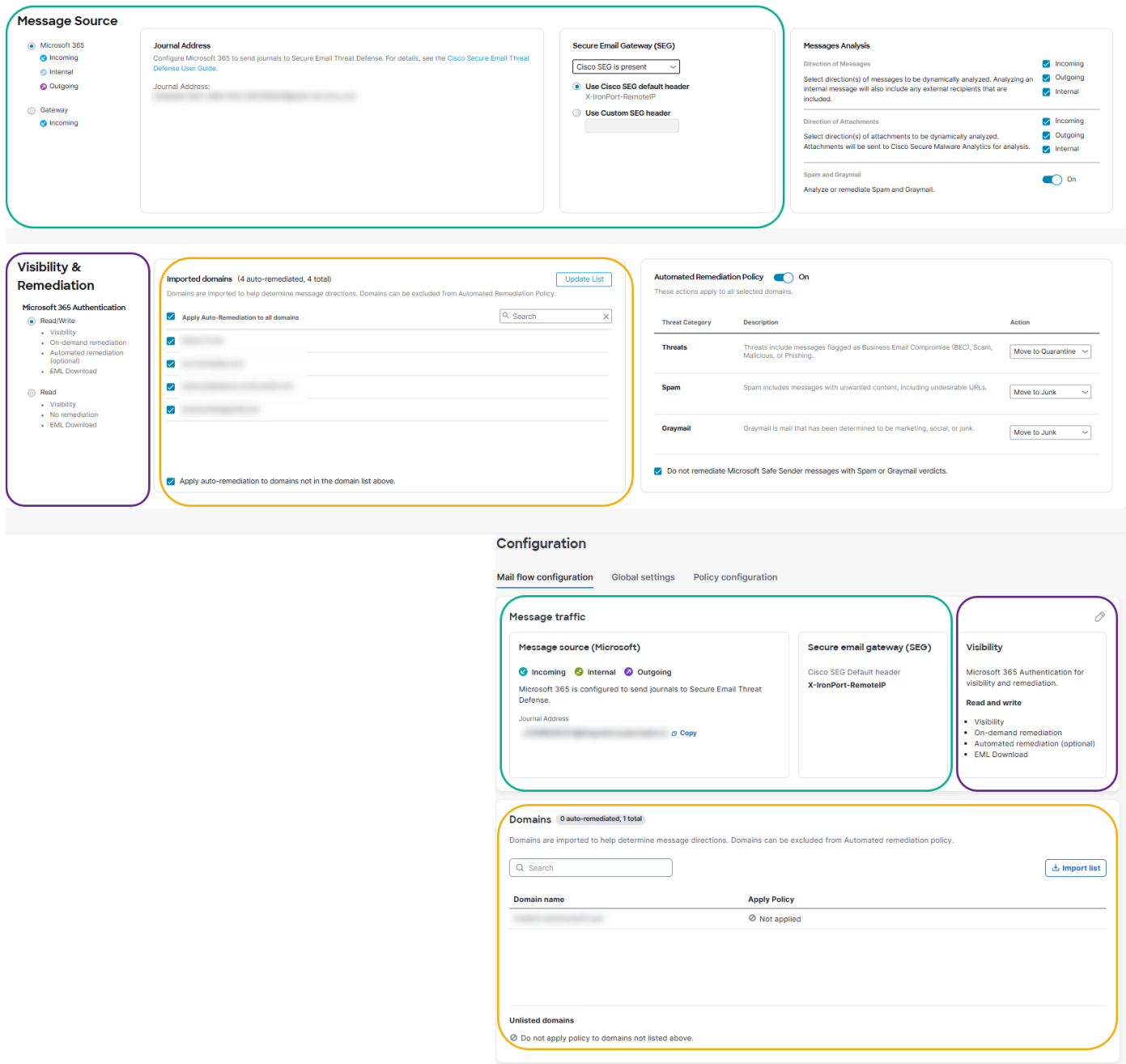

Figure 3.
Policy page settings moved to Mail flow configuration page

Global settings

The Global settings page is where you can view and configure analysis settings for content and attachments and indicate and whether you want to analyze unwanted messages such as Spam and Graymail.

Figure 4.
Message Analysis is moved to the Global settings page

Policy configuration

Automated Remediation Policy settings are accessible from the Policy configuration page. This new page introduces the concept of a Base Policy.

Exceptions to the Base Policy can be created in the form of Allow List, Verdict Override, and Bypass Analysis rules. More policy exceptions will be added in future releases.
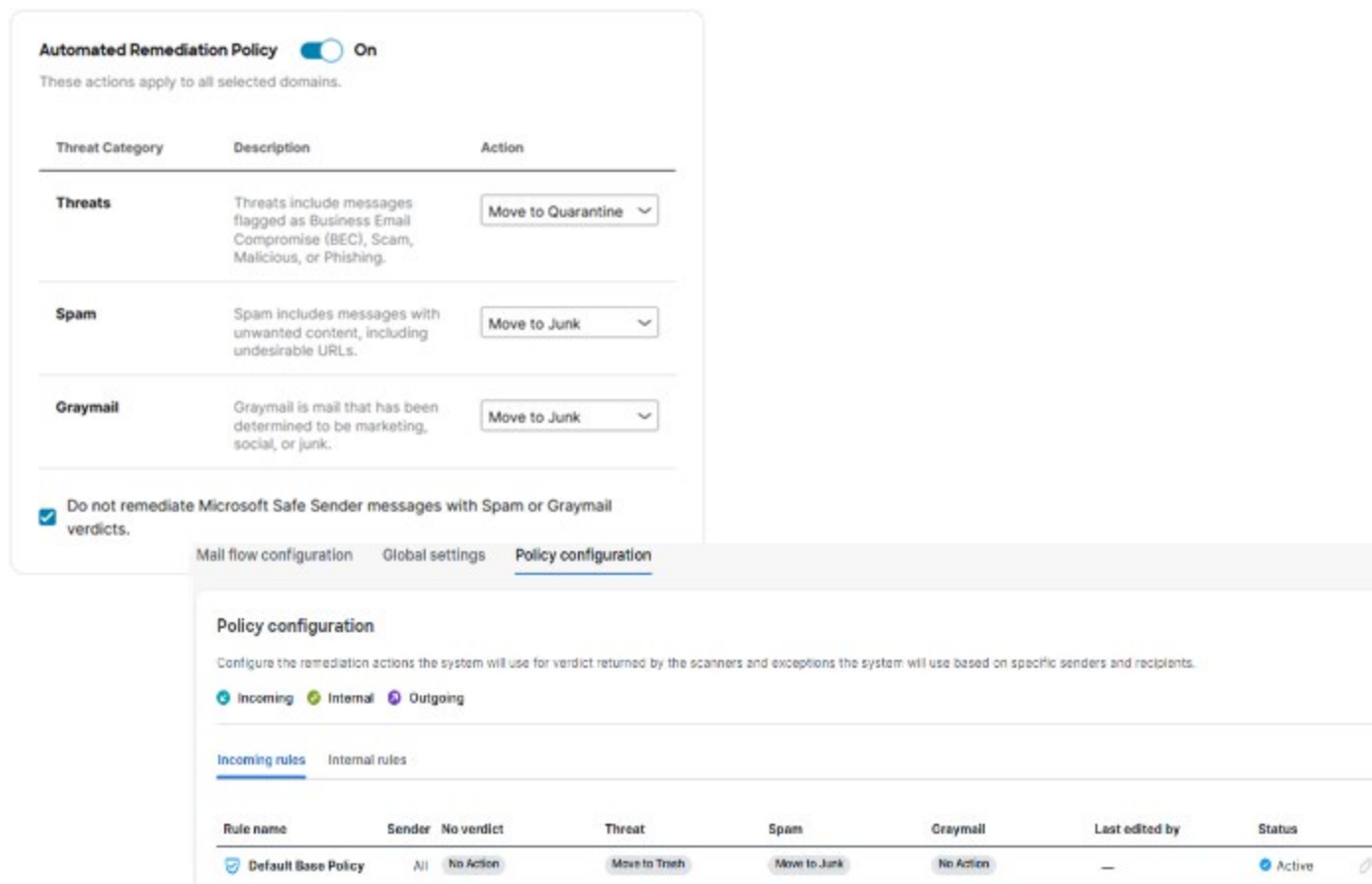
Figure 5.
Automated Remediation policy settings are replaced by Default Base Policy settings on the Policy configuration page

Edit the policy by clicking the pencil icon next to the Default Base Policy row. You can set different policies by message direction. Internal message settings also apply to outgoing messages in a sender's mailbox. For example, if bob@yourcompany.com sends a message to a recipient outside of your domain, the Internal message settings apply to the message in his sent messages folder.

Figure 6.
Edit Default Base Policy dialog where you can set remediation policy by direction

More to Come

Additions to the Configuration pages are currently being developed. These will include new Policy exceptions to allow blocking some message sources. Stay tuned for more updates as they become available.