

# Configure Sender Domain Exception List for Secure Email Gateway

## Contents

---

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Overview](#)

[Configure](#)

[Verify](#)

[Troubleshoot](#)

[Related Information](#)

---

## Introduction

This document describes "New Changes," to the Sender Domain Reputation (SDR) setting option Domain Exception List, for Cisco Secure Email Gateway (SEG).

Contributed by Chris Arellano Cisco TAC Engineer.

## Prerequisites

A general knowledge of the SEG settings and configuration is desired.

AsyncOS 15.0 and newer for Cisco Secure Email Gateway (SEG).

General understanding of the SDR Feature.

## Requirements

Enable Sender Domain Reputation Service and create an Address List with the Domain Only option.

## Components Used

- The information in this document is based on these software and hardware versions:
  - Cisco Secure Email Gateway (SEG) AsyncOS 15.5.1 and newer.
- SEG Sender Domain Reputation.
- Address List.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

## Overview

Sender Domain Reputation is a cloud service that collects multiple sender values, derives verdicts and provides options to take action on those verdicts. SDR allows settings to bypass trusted domains through the use of an Address List applied to the Domain Exception List.

The SDR Domain Exception List in AsynOS releases prior to SEG 15.0 had 2 options:

- Enabled = Match the Envelope From, domain to bypass SDR action.
- Disabled = Match only if all are present: Envelope-from + Friendly From + Reply-To + SPF + DKIM + DMARC .

The Domain Exception List for SEG 15.0 and newer options:

- Enabled = Match the Envelope From, domain to bypass SDR action.
- Disabled = Match if the domain is present in any of the values:
  - HELO
  - RDNS
  - Envelope From
  - From
  - Reply-To

## Configure

The focus of this article is the new Domain Exception List configuration only. The full SDR setup and configuration are provided within the User Guide.

Navigate within the WebUI to **Security Services > Domain Reputation**.

- The option **Match Domain Exception List based on the Domain Name portion of the Envelope From** is enabled by default.
  - If the Checkbox is enabled, only the value "Envelope From, header" will match and bypass the message if convicted.
  - If the Checkbox is blank, SDR Domain Exception List will match any of these header fields 'HELO:', 'RDNS:', 'Envelope From:', 'From:' and 'Reply-To:' headers, will match and bypass the message if convicted.


If the associated ? informational icon is selected the setting details are presented.

**Match Domain Exception List based on Domain in Envelope From.** ✕

Disable this option if you want to skip the SDR checks if any domains in the 'HELO:', 'RDNS:', 'Envelope From:', 'From:' and 'Reply-To:' headers of the message match the domains configured in the domain exception list.

**Note:** By default, SDR checks are skipped based on the domain in the 'Envelope From:' header only.

---

 **Note:** By default, SDR checks are skipped based on the domain in the 'Envelope From:' header only.

---


Select **Edit Global Settings** to remove the checkbox option, as shown in the image:

**Sender Domain Reputation Overview**

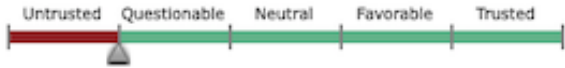
**Enable Sender Domain Reputation Filtering**

Include Additional Attributes:  Enable

Sender Domain Reputation Query Timeout:  seconds

Match Domain Exception List based on Domain in Envelope From:  Enable 

Action applied on Message based on SDR Verdict:  Reject  Accept



For Threat Level Unknown:  Accept  Reject

The Domain Exception List itself is an Address List containing domain names.

## Verify

To verify proper function using the new Disable functionality you require a test message sent to the SEG with a matching domain value in one of the 5 header values.

A sample log indicating an exception within the Global Exception List and matched within a Mail Flow Policy would present in the early stage to the mail\_logs:

```
Info: MID 14 SDR: MID 14 containing domain name'test1.example.com' matched the global domain exception
```

A sample log indicating an exception would contain both the domain and the exception list name.

```
Info: MID 16 containing domain name 'test3.example.com' matched the domain exception list 'SDR-TEST-3'
```

## Troubleshoot

If questions arise as to the accuracy of a selected message verdict, the values are documented and compared against the message tracking.

- Document the Global **Domain Reputation Settings** > **Security Settings** > **Domain Reputation**.
- Verify the associated Address List configured in the Global Domain Reputation Settings.
- Verify the matching Mail Flow Policy based on the message tracking.
- Check and note details of any Message Filters or Content Filters with Domain Exception Lists configured.

Collect Message Tracking, mail logs, and the original email headers.

- If the Global exception matches on a message, there are no log entries for Domain Reputation, simply a line indicating the matched domain.
- If the Global Exception List does not match on a message, there are log entries for Domain Reputation from which to compare values.

- Info: MID 16 SDR: Domains for which SDR is requested: **reverse DNS host:** Not Present, **helo:** mail1.example.com, **env-from:** test2.example.com, **header-from:** te destination.example.com, **reply-to:** test2.example.com
- The email headers include any of the 5 values present in an individual email to compare to the settings.

Once all of the data is collected check for matches or absence of matches to determine proper functionality.

## Related Information

- [Email Security Setup Guide](#)
- [Cisco Secure Email Gateway Launch Page to Support Guides](#)