

# Configure Sender Domain Reputation for ESA

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[Configure](#)

[Enable Domain Reputation Service WebUI](#)

[Domain Exception List](#)

[Create an Address List](#)

[Apply the Address List to the SDR Global Domain Exception List](#)

[Apply the Address List to Content/Message Filters](#)

[Create a Content Filter to Take Action on the SDR Verdict](#)

[Configure SDR through the Use of Message Filters](#)

[Verify](#)

[Troubleshoot](#)

[Related Information](#)

## Introduction

This document describes the Sender Domain Reputation (SDR) configuration for the Email Security Appliance (ESA).

## Prerequisites

### Requirements

Cisco recommends that you have knowledge of these topics:

- ESA concepts
- ESA configuration

### Components Used

The information in this document is based on AsyncOS for ESA 12.0 and later.

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.

## Background Information

1. SDR has been developed as an additional resource in order to improve spam detection.
2. SDR captures multiple header values, uploads them to Talos Threat Intelligence Servers where additional detail gets combined to determine a verdict for each message on a graduated scale based on a formula derived by Talos.acron.

3. The header values included in the decision are:

- Envelope From
- From
- Reply-To
- dmarc, dkim and spf verification (if configured)
- From (name portion) is optionally submitted from the 'From' and 'Reply-To' headers
- Sender IP
- Display name in the 'From' and 'Reply-To' headers

5. SDR Scan gets performed on all inbound messages.

6. SDR scan takes place just after the Simple Mail Transfer Protocol (SMTP) acceptance of a message.

7. No action can be taken without the implementation of a Message Filter or Content Filter.

8. SDR action would take place in a configured Message Filter or Content Filter.

9. Configured components include:

- Enable Domain Reputation Service
- Domain Exception Lists (optional)
  - Domain Exception List (Global)
  - Domain Exception List (Message/Content Filter specific)
- Message Filter or Content Filter

## Configure

### Enable Domain Reputation Service WebUI

SDR can be enabled from either the WebUI or the CLI interfaces.

WebUI:

1. Navigate to **Mail Security Services > Domain Reputation > Enable**.
2. Click the box next to **Enable Sender Domain Reputation Filtering**.
3. Choose this box **Include Additional Attributes: (Optional)** if you would like to include the optional header value to the checked data for improved efficacy. Click ? to learn.
4. Choose this box **Sender Domain Reputation Query Timeout**. Click ? to learn.
5. Choose **Match Domain Exception List based On Domain in Envelope From** - Enabled.
6. Click **Submit > Commit** as shown in the image.

### Domain Reputation



## Domain Reputation

Mode —Cluster: test Change Mode...

Centralized Management Options

### Sender Domain Reputation Overview

<input checked="" type="checkbox"/> Enable Sender Domain Reputation Filtering
Include Additional Attributes: ? <input checked="" type="checkbox"/> Enable
Sender Domain Reputation Query Timeout: ? <input type="text" value="2"/> seconds
Match Domain Exception List based on Domain in Envelope From: ? <input checked="" type="checkbox"/> Enable

Cancel Submit

Domain Reputation" />

Security Services > Domain Reputation

## Domain Exception List

1. The Domain Exception List can bypass Sender Domain Reputation Scanning for inbound mail flow.
2. The Domain Exception List can be applied at different locations in order to affect mail flow.
3. The Global application can apply to all mail scanned.
4. The more detailed application within content/message filters can affect only a configured filter(s).
5. The Domain Exception List provides 2 options to provide both a simple as well as a more secure option.
6. This document describes the options in order to successfully bypass SDR for a message that uses the Domain Exception List.
7. [Domain Exception List Requirements Explained](#)

## Create an Address List

1. Navigate to **Mail Policies > Address List > Add Address List > Name > Description > List Type: Domains Only**
2. Add each domain name with the use of the comma-separated.
3. Click **Submit** and **Commit Changes** as shown in the image.

### Add Address List

**New Address List Details**

Address List Name:	<input type="text" value="SDR_Exception"/>
Description:	<input type="text" value="Domain Exception List"/>
List Type:	<input type="radio"/> Full Email Addresses only <input checked="" type="radio"/> Domains only <input type="radio"/> IP Addresses only <input type="radio"/> All of the above
Addresses:	<input type="text" value="@charees111.com, @cisco.com, @ironport.com"/> e.g.: @example.com, @.example.com

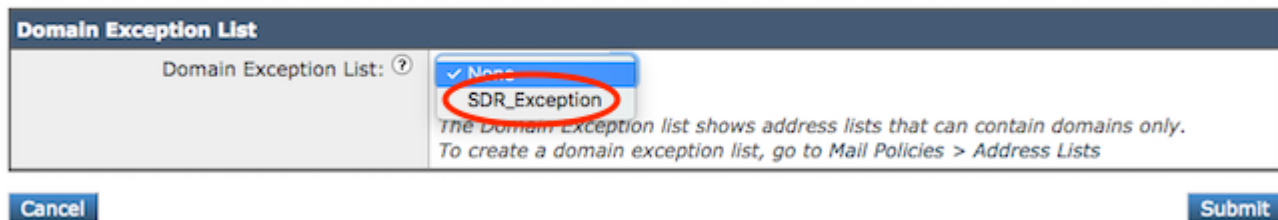
Cancel Submit

Address List to be applied to the Domain Exception List

## Apply the Address List to the SDR Global Domain Exception List

1. Navigate to **Security Services > Domain Reputation > Domain Exception List > Edit Settings > Domain Exception List** (select your list).
2. Click **Submit** and **Commit Changes** as shown in the image.

### Edit Domain Exception List



Choose an Address List from the dropdown

## Apply the Address List to Content/Message Filters

Incoming Content Filters:

1. Navigate to **Condition > URL Reputation > Threat Feeds Option**.
2. Condition Domain Reputation.



Domain Exception List allows per policy action.

Message Filters:

The Domain Exception List application within message filters would be included as an option within a condition.

---

**Note:** These samples include the domain\_exception\_list as a portion of the whole condition.

---

1. sdr-reputation ([ 'awful', 'poor', 'tainted', 'weak', 'unknown', 'neutral', 'good'], **domain\_exception\_list**)
2. sdr-age ("days", <, 5, **domain\_exception\_list**)
3. sdr-unscannable (**domain\_exception\_list**)

A more comprehensive explanation and samples of Message filter application can be found with the [ESA User Guides](#) under the headings:

- Domain Reputation Rule for ETF
- Filtering Messages based on Sender Domain Reputation that uses Message Filter

## Create a Content Filter to Take Action on the SDR Verdict

1. SDR is only enabled for Incoming Mail Flow.
2. The SDR Condition Name: Domain Reputation.
3. Multiple Conditions can be created to combine different results.

4. The Domain Reputation Condition contains 2 different checks that contain multiple options for each:

- Sender Domain Reputation
  - Sender Domain Reputation Verdict
  - Sender Domain Age
  - Sender Domain Reputation Unscannable
- External Threat Feeds
  - Allows the utilization of the Threat Feeds downloaded content lists to scan against the same domain headers collected for SDR.

---

**Note:** These options within the Domain Reputation Condition can visually change based on the different options for each selection.

---

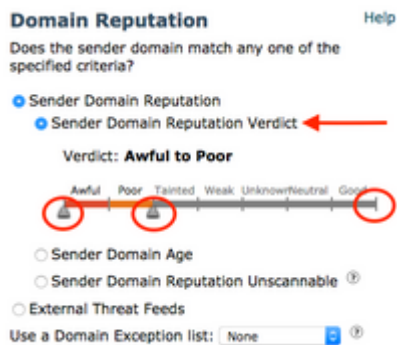
5. The final option within the Domain Reputation Condition is the Domain Exception List.

6. The Domain Exception List function associated with an Address List adds more control to the application of the action by applying the list to the more detailed Mail Policy Level of message processing.

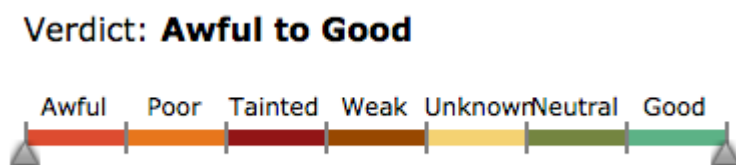
7. Navigate to **Mail Policy > Incoming Content Filters > Add Filter > Add Condition > Domain Reputation**.

8. Condition 1: Sender Domain Reputation Verdict.

- Awful, Poor, Tainted, Weak, Unknown, Neutral, Good
- Contains sliding triangular markers to choose the range you would like to match.
- The Awful and Poor are the recommended values to take action.
- The messages which match Awful and Poor can have an additional Category, value such as Spam or Malicious viewable within Message Tracking.



*SDR Verdict adjustable range slide bar.*



*Full view of the SDR Verdict Slide Bar.*

9. Condition 2: Sender Domain Age.

- The age of the Domain can be associated with more risk or long-established reliability.
- The possibility of a domain with an age of fewer than 10 days can be riskier.

**Domain Reputation** Help

Does the sender domain match any one of the specified criteria?

Sender Domain Reputation

Sender Domain Reputation Verdict

Sender Domain Age ←

- ✓ Greater than
- Greater than or equal to
- Less than
- Less than or equal to
- Equal to
- Does not equal
- Unknown

Day(s) ?

Extension Unscannable ?

Use a Domain Exception list:  ?

*Sender Domain Age. Lower values suggest more risk.*

10. Condition 3: Sender Domain Reputation Unscannable.

- Provide an option for administrators to take action if a verdict cannot be obtained.

**Domain Reputation** Help

Does the sender domain match any one of the specified criteria?

Sender Domain Reputation

Sender Domain Reputation Verdict

Sender Domain Age

→  Sender Domain Reputation Unscannable ?

External Threat Feeds

Use a Domain Exception list:  ?

*SDR Unscannable*

11. Condition 4: External Threat Feeds


- The headers included in SDR Scanning can also be scanned with custom downloaded STIX/TAXII content.
- The External Threat Feeds is covered in more detail here [External Threat Feeds](#)

## Domain Reputation

Help

Does the sender domain match any one of the specified criteria?

Sender Domain Reputation

External Threat Feeds 

Does the domain in the header match the threat information from any one of the selected sources?

Available Sources:


Alienvault  
beta\_taxii  
hat-phish\_tank

Add >

< Remove

Selected Sources:





Select the headers where the reputation of the domain must be checked: 

Envelope Sender

From Header

Reply-to

Other Header 


Use a Domain Exception list:  

*External Threat Feeds can be used to scan the same headers used for SDR*

### [Email Security Appliance User Guides](#)

#### 12. Condition 5: Use Domain Exception List.

- The use of the Domain Exception List within the Content Filter adds more control than the Global List.

Use a Domain Exception list:    
 None  
 SDR\_Exception

*Domain Exception List allows per policy action.*

13. The action combined with these conditions can range from minimal to extreme and it depends on the desired results of the administrator.

14. Some of the more popular actions are listed:

- Quarantine/Copy to Quarantine
- Drop
- Add disclaimer or warning to the subject or body of the message.
- Create a Log Entry to generate a specific word, phrase, or value to the message tracking logs.

## Configure SDR through the Use of Message Filters

1. The [ESA User Guides](#) is an excellent source for Message Filter syntax, definitions, and examples.
2. Search for this heading in the User Guide for additional content for Message Filters beyond the information provided here.

- Filtering Messages based on Sender Domain Reputation with Message Filter

3. These conditions are associated with SDR Message Filter:

- if sdr-reputation (['awful', 'poor'] >>> all values for this include: Awful, Poor, Tainted, Weak, Unknown, Neutral, Good
- if sdr-reputation (['awful', 'poor'], "<domain\_exception\_list>") >>> This includes the use of a Domain Exception List
- if sdr-age (<â€~unit>, <â€~operator> <â€~actual valueâ€™™>) >>> Reference the User Guide for "operator" definition.
  - if (sdr-age ("unknown", "")) >>> unit = unknown. Remaining values are replaced with the ""
  - example: if (sdr-age ("months", <, 1, "")). >>> unit = days, months, years. Operator = < (less than). Actual Value = 1
- if sdr-unscannable (<'domain\_exception\_list'>) >>> As presented, if the message results in unscannable. This sample includes the domain exception list condition as well.
- if (sdr-unscannable ("")) >>> This sample does not include the Exception list. The value gets replaced with ("")

## Verify

Use this section to confirm that your configuration works properly.

Once the SDR Service has been enabled, the mail\_logs and Message Tracking begin to show the SDR: log entries.

1. mail\_logs contain the score of the SDR data collected.
2. The score is determined early in the mail flow, prior to determining the Mail Policy.
3. Actions taken on the verdict occur at the time of the message filter and content filter actions.

```
<#root>
```

```
xxx.com>
```

```
mail_logs sample including SDR verdict
```

```
Tue Dec 3 15:22:44 2019 Info: New SMTP ICID 5539460 interface Data 1 (10.10.10.170) address 55.1.x.y rev
Tue Dec 3 15:22:44 2019 Info: ICID 5539460 ACCEPT SG Production_INBOUND match xxx1.xxx.com SBRS 2.5 cour
Tue Dec 3 15:22:44 2019 Info: ICID 5539460 TLS success protocol TLSv1.2 cipher ECDHE-RSA-AES128-GCM-SHA2
Tue Dec 3 15:22:44 2019 Info: Start MID 3291517 ICID 5539460
Tue Dec 3 15:22:44 2019 Info: MID 3291517 ICID 5539460 From: <customer@xxx.com>
Tue Dec 3 15:22:44 2019 Info: MID 3291517 ICID 5539460 RID 0 To: <owner@xxx.com>
Tue Dec 3 15:22:44 2019 Info: MID 3291517 IncomingRelay(PROD_TO_BETA): Header Received found, IP 172.20.
Tue Dec 3 15:22:44 2019 Info: MID 3291517 Message-ID '<mail>'
Tue Dec 3 15:22:44 2019 Info: MID 3291517 Subject "You\\'ve Been Nominated for inclusion with Who\\'s WH
```



```

Tue Dec 3 15:22:44 2019 Info: MID 3291517 SDR: Domains for which SDR is requested: reverse DNS host: Not
Tue Dec 3 15:22:46 2019 Info: MID 3291517 SDR: Consolidated Sender Reputation: Awful, Threat Category: M
Tue Dec 3 15:22:46 2019 Info: MID 3291517 SDR: Tracker Header : 5Zrl76622ZDGPsS6cByUUXq7LTXXS3/wonoZb5c
Tue Dec 3 15:22:46 2019 Info: MID 3291517 ready 10011 bytes from <owner@xxx.com>
Tue Dec 3 15:22:46 2019 Info: MID 3291517 Custom Log Entry: MF_URL_Category_all HIT
Tue Dec 3 15:22:46 2019 Info: MID 3291517 matched all recipients for per-recipient policy DEFAULT in the
Tue Dec 3 15:22:47 2019 Info: MID 3291517 interim verdict using engine: CASE spam positive
Tue Dec 3 15:22:47 2019 Info: MID 3291517 using engine: CASE spam positive
Tue Dec 3 15:22:47 2019 Info: MID 3291517 interim AV verdict using Sophos CLEAN
Tue Dec 3 15:22:47 2019 Info: MID 3291517 antivirus negative
Tue Dec 3 15:22:47 2019 Info: MID 3291517 AMP file reputation verdict : SKIPPED (no attachment in messag
Tue Dec 3 15:22:47 2019 Info: MID 3291517 using engine: GRAYMAIL negative
Tue Dec 3 15:22:47 2019 Info: MID 3291517 Custom Log Entry: SDR_Verdict_matched_Awful_Poor
Tue Dec 3 15:22:47 2019 Info: Start MID 3291519 ICID 0

```

4. Simple grep commands in order to check the frequency of, or existence of, specific verdicts.

- >> grep "Sender Reputation: Awful" mail\_logs
- >> grep "Sender Reputation: Poor" mail\_logs

5. Further, mail log details can be obtained with the use of the CLI **findevent** command in conjunction with the MID value.

```

xxx.com> grep "SDR: Domain Reputation.*Poor" mail_logs
Tue Dec 3 11:07:01 2019 Info: MID 3265844 SDR: Consolidated Sender Reputation: Poor, Threat Category: Sp
Tue Dec 3 12:57:28 2019 Info: MID 3277401 SDR: Consolidated Sender Reputation: Poor, Threat Category: Sp

```

```

xxx.com> grep "SDR: Domain Reputation.*Awful" mail_logs
Tue Dec 3 10:24:08 2019 Info: MID 3261075 SDR: Consolidated Sender Reputation: Awful, Threat Category: M
Tue Dec 3 15:18:27 2019 Info: MID 3291182 SDR: Consolidated Sender Reputation: Awful, Threat Category: M

```

## Troubleshoot

This section provides information you can use to troubleshoot your configuration.

1. No SDR: logs present within the mail\_logs or Message Tracking:

- SDR logs can always be present for messages which pass through an ACCEPT Mail Flow Policy.
- Ensure the Service has been enabled as presented in the initial steps of this guide.

2. SDR Timed Out:

- Verify the Cisco cloud server for SDR is open and available for use.
- v2.sds.cisco.com

- A very general test can be performed with the use of the telnet from the CLI.
- If the banner appears, it can confirm the basic reachability.
  - **CLI > telnet v2.sds.cisco.com 443** (this can verify a point in time only.)
- Check logs from other services to determine if there are potential communication failures out to internet-based services.
- **CLI > displayalerts** in order to check for additional signs of communication failures.
- Prior to 13.5 AsyncOS, SDR and URL Filtering both utilize v2.sds.cisco.com.
  - A check of the **URL Filtering CLI command > websecuritydiagnostics** can provide some validation if the network path contains latency.
- Check the **Sender Domain Reputation Timeout Setting**, and determine if the value can be increased 1-10 seconds. Navigate to **Security Services > Domain Reputation > Edit > Sender Domain Reputation Query Timeout:2**
- The default is 2 seconds and a maximum setting of 10 seconds.

## Related Information

- [ESA User Guides](#)
  - [ESA Release Notes](#)
  - [ESA CLI Reference Guides](#)
  - [Technical Support & Documentation - Cisco Systems](#)
-