How to Bypass DMARC Check on Email Security Appliance

Contents

Introduction

This document describes how to bypass Domain-based Message Authentication, Reporting and Conformance (DMARC) check on Email Security Appliance (ESA). Refer to Introduction about Email Authentication.

Verify DMARC

DMARC is a technical specification created to reduce the potential for email-based abuse. DMARC standardizes how email receivers perform email authentication with the use of Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM) mechanisms. In order to pass DMARC verification, an email must pass at least one of these authentication mechanisms, and the Authentication Identifiers must comply with RFC 5322.

The appliance allows you to:

- Verify incoming emails with the use of DMARC.
- Define profiles to override (accept, quarantine, or reject) domain owners' policies.
- Send feedback reports to domain owners, which helps to strengthen their authentication deployments.
- Send delivery error reports to the domain owners if the DMARC aggregate report size exceeds 10 MB or the size specified in the aggregated reports (RUA) tag of the DMARC record.

AsyncOS can handle emails that are compliant with the DMARC specification as submitted to Internet Engineering Task Force (IETF) on March 31, 2013. For more information, see http://tools.ietf.org/html/draft-kucherawy-dmarc-base-02.

> **Note**: The appliance will not perform DMARC verification of messages from domains with malformed DMARC records. However, the appliance can receive and process such messages.

Configure DMARC Bypass

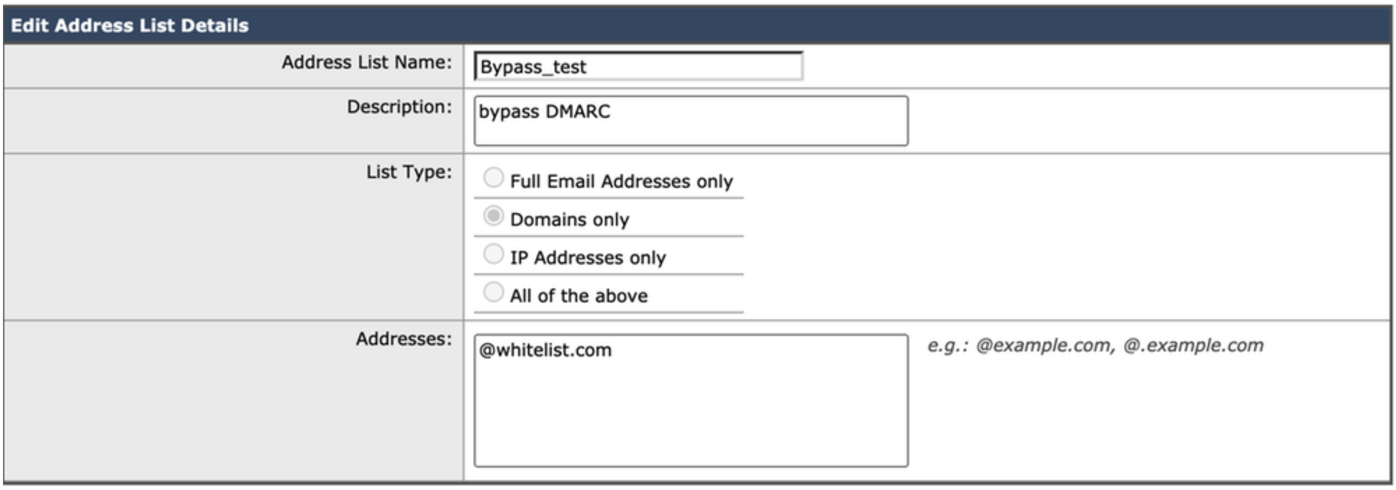
If as an admin your requirement is to skip DMARC verification of messages from specific senders, you will have to follow few steps to achieve the bypass successfully. An overview of the steps can be referred to here:

> **Note**: Address lists that are created with the use of full email addresses or domains only can be used to bypass DMARC verification. You can use an **Address List** with the option **All of the above**. However, entries with only domain/full email address or partial domain address will work for an exception. You will have to use the **domain/full email address** mentioned in the **From** header.

1. Ensure **DMARC Verification** is turned **ON** for the associated Mail Flow Policy.
2. Navigate to **Mail Policies > Address List**.
3. Click on **Add Address List**.
4. Create an **Address List** by filling in the details.
5. Click on **Submit**.
6. Once the **Address List** is created you will have to call the list to **DMARC Specific Senders Bypass Address List**.

Here is an example of how the bypass configuration can be configured and how logging will be done:

The address list is created with "**Domains only**" as an example and added in the **From** header details.



Edit Address List Details

Address List Name: Bypass_test

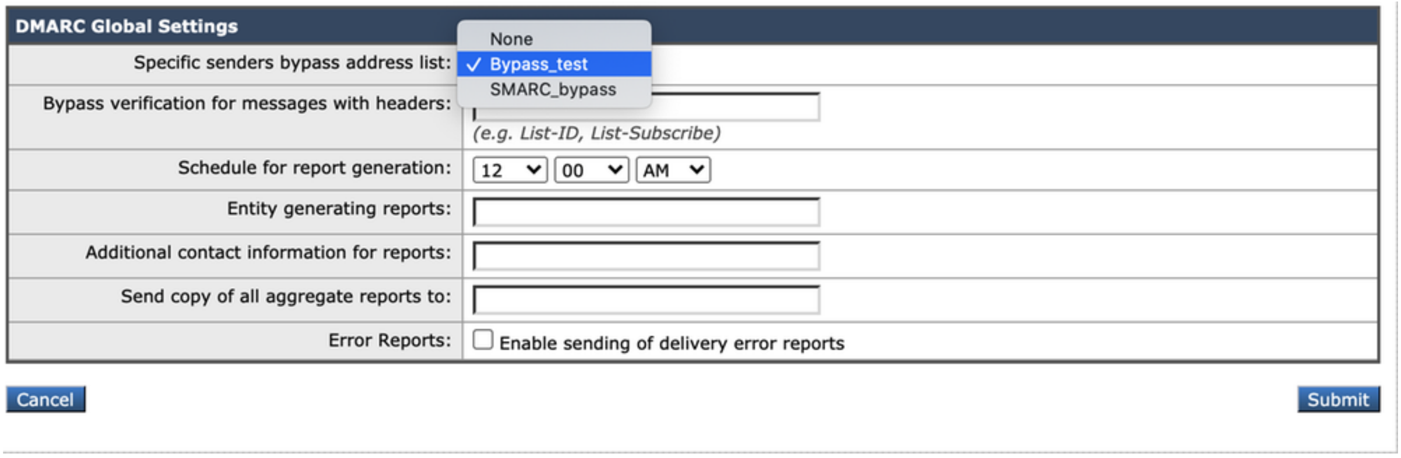
Description: bypass DMARC

List Type:
○ Full Email Addresses only
● Domains only
○ IP Addresses only
○ All of the above

Addresses: @whitelist.com

e.g.: @example.com, @.example.com

Once your address list is successfully created with all the desired entries, you will have to call the **Address List** under your **DMARC Specific Senders Bypass Address List**. You will need to navigate to **Mail Policies > DMARC > Edit Global Settings** and call your newly created **Address List** by clicking on the dropdown, as shown here:



DMARC Global Settings

Specific senders bypass address list:	None ✓ Bypass_test SMARC_bypass
Bypass verification for messages with headers:	(e.g. List-ID, List-Subscribe)
Schedule for report generation:	12 00 AM
Entity generating reports:	
Additional contact information for reports:	
Send copy of all aggregate reports to:	
Error Reports:	□ Enable sending of delivery error reports

Difference in Mail_Logs

A representation of the mail_logs is presented here which will help in understanding the difference between logging, when a domain's DMARC is validated and when it is configured to skip.

Mail Logs when DMARC is checked:

```
Sat Mar 20 21:14:22 2021 Info: ICID 57 ACCEPT SG UNKNOWNLIST match sbrs[none] SBRS rfc1918
country not applicable

Sat Mar 20 21:14:22 2021 Info: Start MID 76571 ICID 57

Sat Mar 20 21:14:22 2021 Info: MID 76571 ICID 57 From: <itrustyou@whitelist.com>

Sat Mar 20 21:14:22 2021 Info: MID 76571 ICID 57 RID 0 To: <abc@iaccceptyou.com>

Sat Mar 20 21:14:23 2021 Info: MID 76571 DMARC: Verification skipped (No record found for the
sending domain)

Sat Mar 20 21:14:23 2021 Info: MID 76571 DMARC:

Sat Mar 20 21:14:23 2021 Info: MID 76571 Message-ID '<613a1e1b-998a-6375-8887-
ab2c6d430256@whitelist.com>'

Sat Mar 20 21:14:23 2021 Info: MID 76571 Subject 'Test 4'
```

> **Note**: There is no record published for the domain @whitelist.com, which is the reason why we see "No record found for the sending domain".

Mail Logs for Bypass DMARC Check

```
Sat Mar 20 21:15:36 2021 Info: ICID 58 ACCEPT SG UNKNOWNLIST match sbrs[none] SBRS rfc1918
country not applicable

Sat Mar 20 21:15:37 2021 Info: Start MID 76572 ICID 58

Sat Mar 20 21:15:37 2021 Info: MID 76572 ICID 58 From: <itrustyou@whitelist.com>

Sat Mar 20 21:15:37 2021 Info: MID 76572 ICID 58 RID 0 To: <abc@iacceptyou.com>

Sat Mar 20 21:15:37 2021 Info: MID 76572 DMARC: Verification skipped (Local bypass
configuration)

Sat Mar 20 21:15:37 2021 Info: MID 76572 Message-ID '<2ba742a2-f8ba-9ff0-7dc9-
362421f5177e@whitelist.com>'

Sat Mar 20 21:15:37 2021 Info: MID 76572 Subject 'Test Bypass DMARC'
```

Related Information

- Understanding DMARC workflow
- How to Verify Incoming Messages Using DMARC
- Filter to handle messages that skipped DMARC verification
- Technical Support & Documentation - Cisco Systems