Verify Sender Domain Reputation change on 14.2.0 AsyncOS upgrade

Contents

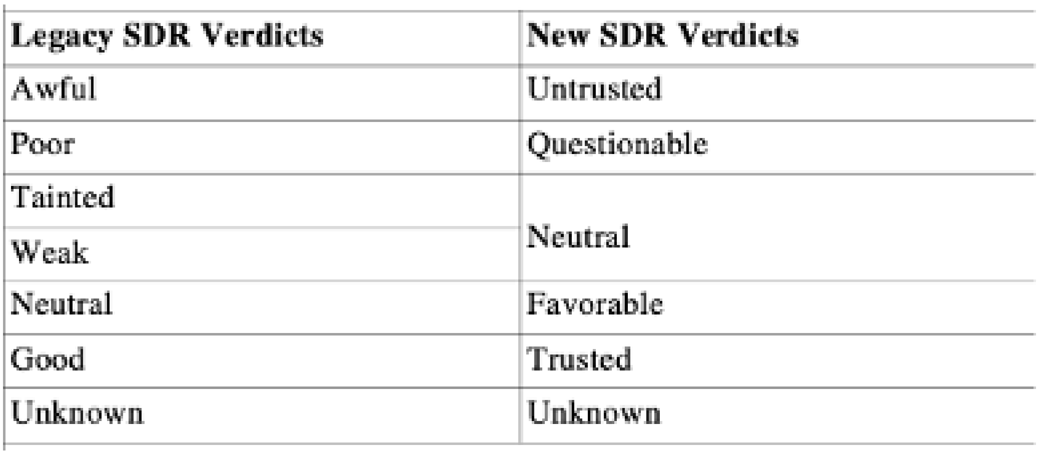
Introduction

This document describes the changes in for Sender Domain Reputation (SDR) on the Secure Email platform for on-premise, virtual environment (ESA), and cloud environment (CES).

Q. What are the changes made on SDR AsyncOS 14.2.0?

> **Warning**: **SDR configurations of Reject action for Tainted and/or Weak Verdicts are automatically changed on upgrade to 14.2. The configuration changes the ESA SDR configuration to reject at Neutral Threat Level.**

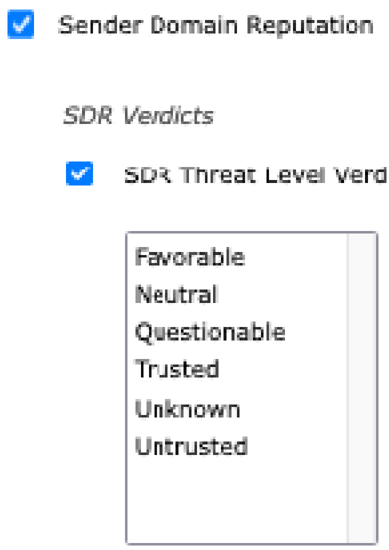
1) SDR Legacy Verdicts change of verdicts now named **Threat Levels**, as shown in the image:



Legacy SDR Verdicts	New SDR Verdicts
Awful	Untrusted
Poor	Questionable
Tainted	Neutral
Weak	
Neutral	Favorable
Good	Trusted
Unknown	Unknown

> **Note**: This is a change in SDR scan behavior with a different verdict decision mechanism. You must not expect the verdict to match the old solution for every set of sender information.

2) 'Message Tracking' by the advanced condition of SDR is replaced with the list shown:



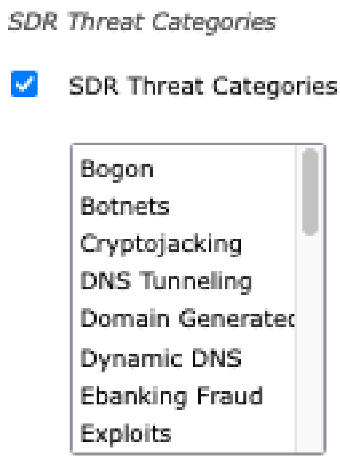
☑ Sender Domain Reputation

SDR Verdicts

☑ SDR Threat Level Verdicts

Favorable
Neutral
Questionable
Trusted
Unknown
Untrusted

3) SDR Threat Category **Banking Fraud** is changed to **Ebanking Fraud**, as shown in the image:



SDR Threat Categories

☑ SDR Threat Categories

Bogon
Botnets
Cryptojacking
DNS Tunneling
Domain Generatec
Dynamic DNS
Ebanking Fraud
Exploits

> **Note**: **All Untrusted** does not have a category listed, however SDR categories such as, '*spam*,' '*malicious*,' etc, are flagged as either **Untrusted** or **Questionable**.

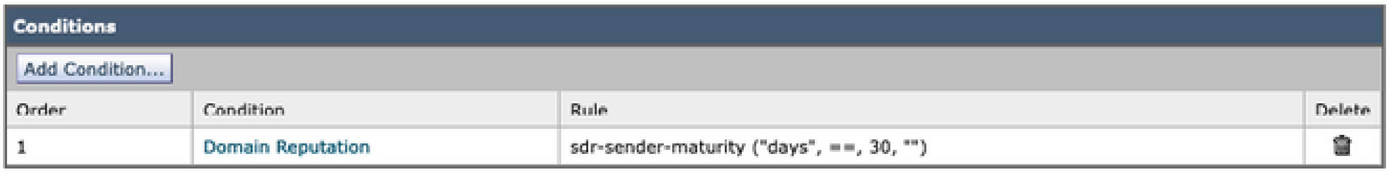
4) mail_logs contains an additional log line for SDR verdicts, it is written after **From** logline if the senders reputation is not rejected. A second SDR line appears in the mail logs.

```
Info: Start MID 11 ICID 19884
Info: MID 11 ICID 19884 From: test@cisco.com
Info: MID 11 SDR: Domains for which SDR is requested: reverse DNS host: Not Present, helo:
desktop-9pf6f2t, env-from: cisco.com, header-from: Not Present, reply-to: Not Present
Info: MID 11 SDR: Consolidated Sender Threat Level: Favorable, Threat Category: N/A, Suspected
Domain(s) : N/A (other reasons for verdict). Sender Maturity: 30 days (or greater) for domain:
cisco.com
Info: MID 11 ICID 19884 RID 0 To: test@cisco.com
Info: MID 11 Message-ID 'op.1m7bljjr8qfre9@desktop-9pf6f2t'
Info: MID 11 Subject "test 1"
Info: MID 11 SDR: Domains for which SDR is requested: reverse DNS host: Not Present, helo:
desktop-9pf6f2t, env-from: cisco.com, header-from: cisco.com, reply-to: Not Present
Info: MID 11 SDR: Consolidated Sender Threat Level: Favorable, Threat Category: N/A, Suspected
Domain(s) : N/A (other reasons for verdict). Sender Maturity: 30 days (or greater) for domain:
cisco.com
Info: MID 11 SDR: Tracker Header :
629d04c8_DDZqM4buLke8/Do4MqUGdJEP9QZc73Ofsh9YLwqvKidy3M/WEb0fkQpwOOtRVhrhSJWgCv2NjL/JQMsjH5QzZw=
=
```

5) SDR configured to reject in the global settings occurs at the envelope phase of the SMTP conversation which is just after the envelope from the header is sent and no other data is sent yet.

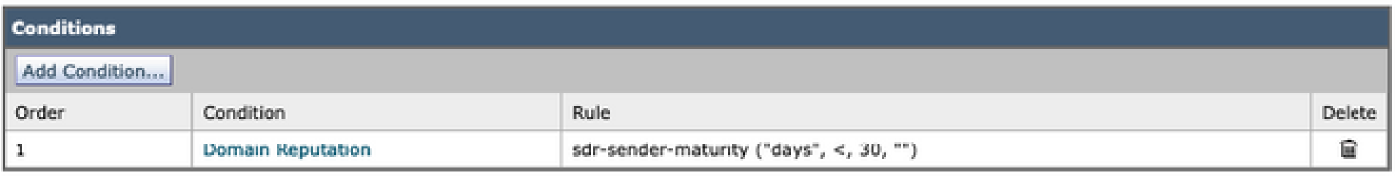
```
Info: Start MID 9364 ICID 79
Info: MID 9364 ICID 79 From: <test@incomingtest.contentfilter.com>
Info: MID 9364 SDR: Domains for which SDR is requested: reverse DNS host: Not Present, helo:
mail.cisco.com, env-from: lana.cf, header-from: Not Present, reply-to: Not Present
Info: MID 9364 SDR: Consolidated Sender Threat Level: Untrusted, Threat Category: N/A, Suspected
Domain(s) : lana.cf. Sender Maturity: 1 day for domain: lana.cf
Info: MID 9364 ICID 79 Receiving Failed: Message rejected by Sender Domain Reputation engine
Info: MID 9364 SDR: Tracker Header :
629d5de5_JxmxzLXzbSob4h6Tqmxj2QFeN6eeb3J8CJ2zj9h8XgF/+e0YQVxd05lnVSwX9Gh37ISaiDHc0SJ5eRdyLYasmQ=
=
Info: MID 9364 Subject ""
Info: Message aborted MID 9364 Receiving aborted
Info: Message finished MID 9364 aborted
```

6) Due to the expected behavior explained as provided on 'Cisco bug ID CSCwb32685' and here Field Notice: FN - 72389 - Cisco Secure Email Gateway: Talos Domain Age Update you must not use the three conditions in your filters: **less than**, **equal to**, and **less than and equal to**, otherwise all the domains that hit the policy or policies matches the conditions, as shown in the image:



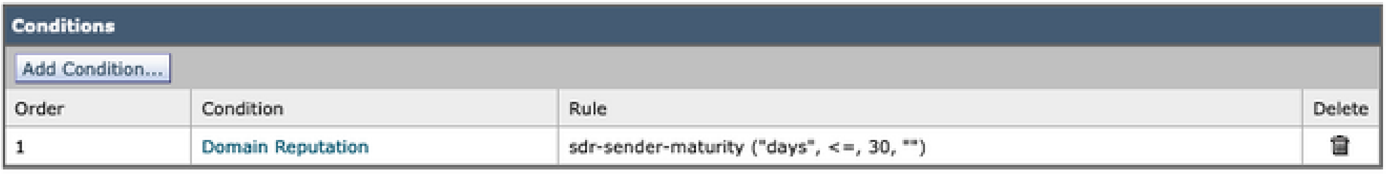
Conditions

Order	Condition	Rule	Delete
1	Domain Reputation	sdr-sender-maturity ("days", ==, 30, "")	🗑



Conditions

Order	Condition	Rule	Delete
1	Domain Reputation	sdr-sender-maturity ("days", <, 30, "")	🗑



Conditions

Order	Condition	Rule	Delete
1	Domain Reputation	sdr-sender-maturity ("days", <=, 30, "")	🗑

Note: Sender Maturity is set to a limit of 30 days, and beyond this limit, a domain is considered mature as an email sender, and no further details are provided.

Related Information

Cisco Secure Email AsyncOS 14.2 Release notes.

Cisco Secure Email and Web Manager AsyncOS 14.2 Release notes.

Field Notice: FN - 72389 - Cisco Secure Email Gateway: Talos Domain Age Update