# Vérifier la modification de la réputation du domaine de l'expéditeur sur la mise à niveau AsyncOS 14.2.0

## Contenu



## Introduction

Ce document décrit les modifications apportées à pour la réputation de domaine de l'expéditeur (SDR) sur la plate-forme de messagerie sécurisée pour l'environnement sur site, l'environnement virtuel (ESA) et l'environnement cloud (CES).

## Q. Quelles sont les modifications apportées à SDR AsyncOS 14.2.0 ?

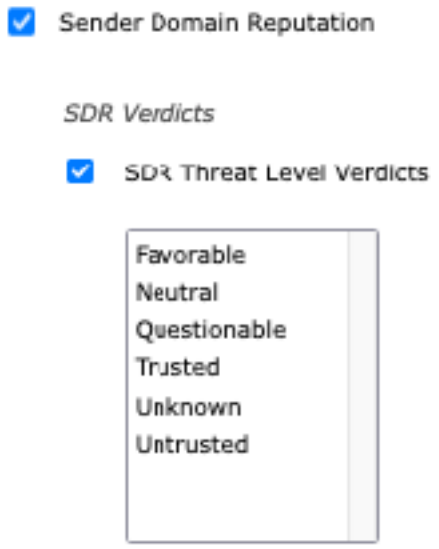
> **Avertissement : Les configurations SDR de l'action Rejeter pour les verdicts tronqués et/ou faibles sont automatiquement modifiées lors de la mise à niveau vers 14.2. La configuration modifie la configuration SDR ESA à rejeter au niveau des menaces neutres.**

**1)** Les anciens verdicts de DTS changent de verdicts maintenant nommés **Niveaux de menace**, comme l'illustre l'image :

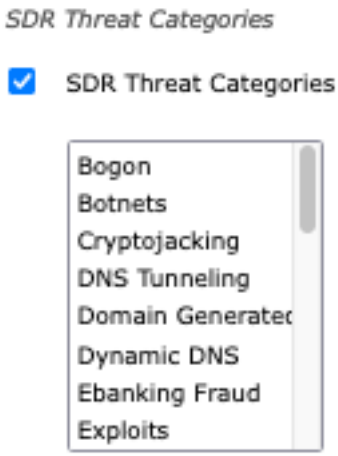
| Legacy SDR Verdicts | New SDR Verdicts |
|---|---|
| Awful | Untrusted |
| Poor | Questionable |
| Tainted | Neutral |
| Weak | |
| Neutral | Favorable |
| Good | Trusted |
| Unknown | Unknown |

> **Note**: Il s'agit d'un changement dans le comportement de l'analyse SDR avec un mécanisme de décision de verdict différent. Vous ne devez pas vous attendre à ce que le verdict corresponde à l'ancienne solution pour chaque ensemble d'informations d'expéditeur.

**2)** 'Suivi des messages' par la condition avancée de SDR est remplacé par la liste affichée :




3) DTS Catégorie de menace **Fraude bancaire** est remplacée par **Fraude bancaire**, comme le montre l'image :




**Note**: **Toutes les catégories non approuvées** ne sont pas répertoriées, mais les catégories de DTS telles que, *spam*, *malveillant*, etc., sont marquées comme **non fiables** ou **douteuses**.

4) mail_logs contient une ligne de journal supplémentaire pour les verdicts SDR, elle est écrite après **From** logline si la réputation des expéditeurs n'est pas rejetée. Une deuxième ligne SDR apparaît dans les journaux de messagerie.

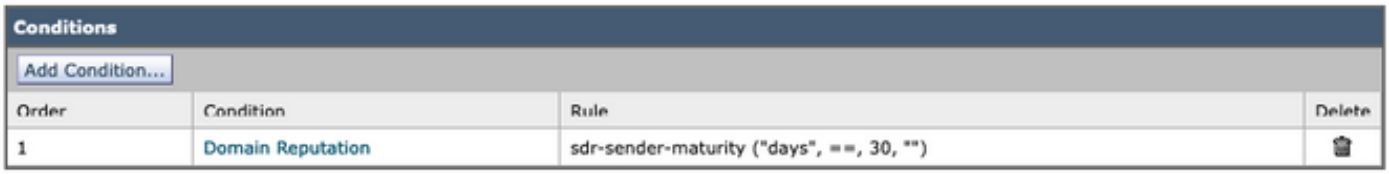
```
Info: Start MID 11 ICID 19884
Info: MID 11 ICID 19884 From: test@cisco.com
Info: MID 11 SDR: Domains for which SDR is requested: reverse DNS host: Not Present, helo:
desktop-9pf6f2t, env-from: cisco.com, header-from: Not Present, reply-to: Not Present
Info: MID 11 SDR: Consolidated Sender Threat 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:
```

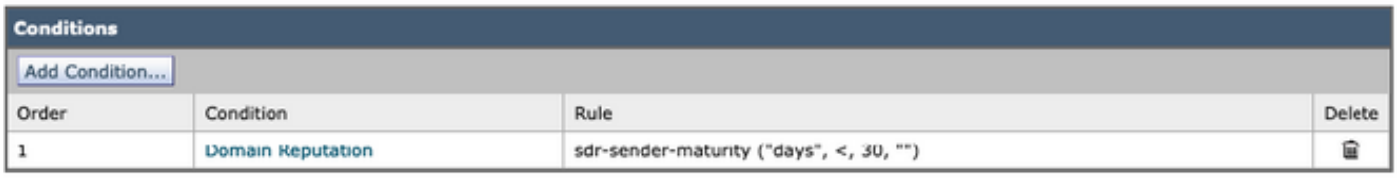
```
cisco.com
Info: MID 11 SDR: Tracker Header :
629d04c8_DDZqM4buLke8/Do4MqUGdJEP9QZc73Ofsh9YLwqvKidy3M/WEb0fkQpwOOtRVhrhSJWgCv2NjL/JQMsjH5QzZw=
=
```

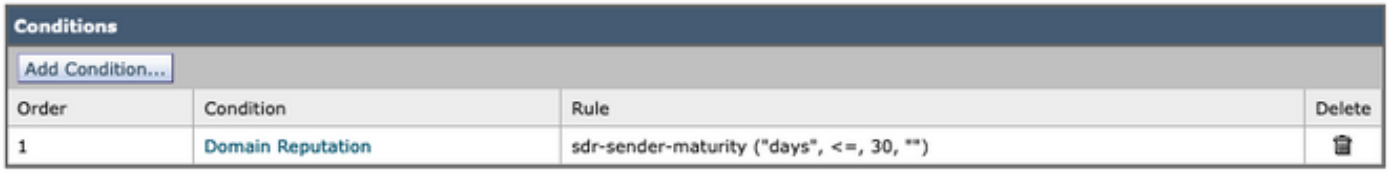
**5)** SDR configuré à rejeter dans les paramètres globaux se produit à la phase enveloppe de la conversation SMTP qui est juste après l'envoi de l'enveloppe de l'en-tête et aucune autre donnée n'est encore envoyée.

```
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)** En raison du comportement attendu expliqué comme indiqué sur 'ID de bogue Cisco CSCwb32685' et ici Avis de champ : FN - 72389 - Passerelle de messagerie sécurisée Cisco : Mise à jour de l'âge du domaine Talos vous ne devez pas utiliser les trois conditions de vos filtres : **inférieur à**, **égal à** et **inférieur et égal à**, sinon tous les domaines qui atteignent la ou les stratégies correspondent aux conditions, comme le montre l'image :




> **Remarque** : la maturité de l'expéditeur est définie sur une limite de 30 jours, et au-delà de cette limite, un domaine est considéré comme mature comme expéditeur de courrier électronique, et aucun détail supplémentaire n'est fourni.

# Informations connexes

Notes de version de Cisco Secure Email AsyncOS 14.2.

Notes de version de Cisco Secure Email and Web Manager AsyncOS 14.2.

Avis sur le champ : FN - 72389 - Passerelle de messagerie sécurisée Cisco : Mise à jour de l'âge du domaine Talos