SALESmanago

Nowe wymogi Gmail i Yahoo

Skonfiguruj SPF, DKIM i DMARC z SALESmanago

Spis treści

1. Dlaczego wdrożenie protokołów SPF, DKIM i DMARC jest konieczne?

Z dniem 1 lutego 2024 r. Gmail oraz Yahoo wprowadziły bardziej rygorystyczną politykę uwierzytelniania dla nadawców wysyłek masowych (tzn. nadawców, którzy co najmniej raz wysłali ponad 5000 e-maili w ciągu jednego dnia). Celem tych nowych wymogów jest ochrona użytkowników przed spamem, phishingiem i złośliwym oprogramowaniem. Oznacza to, że trzy protokoły uwierzytelniania poczty elektronicznej, które do tej pory były jedynie zalecane – SPF, DKIM i DMARC – stają się teraz obowiązkowe (inaczej twoje wysyłki na adresy @gmail.com oraz @yahoo.com mogą zostać zablokowane przez te serwisy pocztowe).

Te trzy protokoły służą następującym celom:

- **SPF (Sender Policy Framework):** określa serwery i domeny uprawnione do wysyłania poczty e-mail w imieniu organizacji.
- **DKIM (DomainKeys Identified Mail):** dodaje podpis cyfrowy do każdej wiadomości wychodzącej, dzięki czemu serwery odbierające pocztę mogą potwierdzić, że wiadomość faktycznie pochodzi z danej organizacji;
- **DMARC (Domain-based Message Authentication, Reporting, and Conformance):** informuje serwery odbierające, co zrobić z wiadomościami wychodzącymi z organizacji, które nie przeszły weryfikacji SPF lub DKIM.

Źródło: Google Help Center (https://support.google.com/a/answer/2466580?hl=pl&sjid=14098442164638657890-EU)

Najprawdopodobniej wymogi te będą mieć zastosowanie do tych klientów SALESmanago, którzy:

- wysyłają e-maile za pośrednictwem SALESmanago (używają konta E-mail Marketing),
- używają zewnętrznego (SMTP) konta wysyłkowego i wysyłają (czy to regularnie, czy sporadycznie) ponad 5000 e-maili dziennie.

Jeżeli nie wiesz, jak wdrożyć te protokoły, zapoznaj się z instrukcjami i objaśnieniami przedstawionymi poniżej.

UWAGA: Przed wdrożeniem protokołu DMARC upewnij się, że dla twojej domeny zostały już wdrożone protokoły SPF oraz DKIM. Bez nich DMARC nie będzie działać poprawnie.

2. Wdrażanie protokołów dla twojej domeny

Protokoły SPF, DKIM i DMARC wdraża się zazwyczaj w ustawieniach **DNS (Domain Name System)** dla twojej domeny. Najprawdopodobniej będziesz w stanie zaimplementować wszystkie te protokoły z pojedynczego miejsca, poprzez dodanie trzech różnych rekordów do ustawień swojej domeny.

UWAGA: Poniższe instrukcje mają charakter ogólny. Rzeczywisty proces może wyglądać inaczej w zależności od platformy eCommerce, rejestratora domen, dostawcy hostingu bądź dostawcy CDN, z których usług korzystasz.

Krok 1. Ustal, gdzie możesz edytować ustawienia DNS.

W zależności od sposobu, w jaki zbudowana jest twoja witryna, rozważ te cztery możliwości:

A. **Sklep internetowy założony na platformie eCommerce** (np. Shopify, BigCommerce): Zaloguj się na swoje konto i znajdź ustawienia DNS. Przykładowo, w Shopify należy przejść do Settings → Domains → Domain settings → Edit DNS settings.
B. **Domena zakupiona za pośrednictwem dostawcy usług hostingowych** (np. OVH, A2 Hosting): Zaloguj się na swoje konto hostingowe i przejdź do panelu sterowania (panelu użytkownika, panelu konfiguracji domeny, itp.).
C. **Domena zakupiona za pośrednictwem rejestratora domen** (np. GoDaddy, OVH): Zaloguj się na konto domeny i przejdź do panelu sterowania (panelu użytkownika, panelu konfiguracji domeny, itp.).
D. **Strona internetowa obsługiwana za pośrednictwem Content Delivery Network (CDN)** (np. Cloudflare): Zaloguj się na swoje konto CDN i przejdź do panelu sterowania (panelu użytkownika, panelu konfiguracji domeny, itp.).
W przypadku Cloudflare, przejdź do DNS → Records (https://developers.cloudflare.com/dns/manage-dns-records/how-to/create-dns-records/).

UWAGA: Jeżeli masz więcej niż jedną domenę, upewnij się, że wybierasz tę, którą chcesz skonfigurować.

Krok 2. Odszukaj właściwe miejsce w ustawieniach DNS.

Po zalogowaniu się na konto umożliwiające edycję ustawień DNS, odszukaj miejsce, w którym możesz **dodawać rekordy dla swojej domeny**. Miejsce to (sekcja, zakładka, itp.) może się nazywać, np.: *Ustawienia DNS* (*DNS settings*), *Edytor stref DNS* (*Zone editor*), *Zarządzanie DNS* (*DNS Management*), *Konfiguracja serwera nazw* (*Name server configuration*) czy też *Zarządzanie rekordami DNS* (*DNS record management*).

Możliwe, że zobaczysz przyciski w rodzaju *Dodaj rekord TXT (Add TXT record)* bądź *Dodaj rekord CNAME* (*Add CNAME record*); możliwe również, że musisz kliknąć przycisk pozwalający dodać rekord, a następnie wybrać rodzaj rekordu z listy. Jeżeli nie możesz znaleźć opcji dodawania rekordu dla swojej domeny, zapoznaj się z artykułami pomocy swojego dostawcy usług (platformy eCommerce, rejestratora domen, dostawcy hostingu, dostawcy CDN) bądź skontaktuj się z jego działem obsługi klienta.

Krok 3. Wdróż protokoły poprzez dodanie rekordów.

Aby wdrożyć wszystkie trzy wymagane protokoły, musisz dodać **cztery rekordy** następujących rodzajów:

Protokół	Rodzaj rekordu
SPF	TXT
DKIM	CNAME **(x2)**
DMARC	TXT

Każdy z tych rekordów wymaga konfiguracji poprzez wprowadzenie następujących wartości:

A. Host (*Nazwa hosta*, *Nazwa*, *Domena; Host record, Host name, Name, Domain,* itp.),
B. Wartość tekstowa (*Wartość główna*, *Rekord*, *Wartość*, *Treść*; *Main value*, *Record*, *Value*, *Content*, itp.), oraz
C. TTL (Time to Live – czas życia).

Ponadto zalecamy **dodanie piątego rekordu, który umożliwi SALESmanago automatyczne zweryfikowanie twojej konfiguracji DKIM**, dzięki czemu oszczędzisz czas (zob. Krok 3.3).

WSKAZÓWKI:

- Po uzupełnieniu pola *Host* możesz zauważyć, że na końcu wprowadzonej wartości została dodana kropka. Nie próbuj jej usuwać – jest to wymagany element formatowania.
- Jeżeli masz wątpliwości, które pole jest polem *Host*, popatrz na istniejące rekordy i sprawdź, które pole zawiera adresy domen.

Zapoznaj się z instrukcjami poniżej i dowiedz się, jak należy wypełnić poszczególne pola, aby zdefiniować nowe rekordy.

UWAGA: Przed wdrożeniem protokołów upewnij się, że nie zostały już wdrożone dla twojej domeny. Prawdopodobnie możesz to sprawdzić w tym samym panelu sterowania/użytkownika/konfiguracji, w którym możesz dodać nowy rekord – po prostu sprawdź listę istniejących rekordów.

Pamiętaj, że rekord SPF może wymagać aktualizacji – zobacz instrukcje poniżej.

Krok 3.1. Dodawanie protokołu SPF

Dodaj **rekord TXT** dla swojej domeny.

Prawdopodobnie zobaczysz kilka pól wprowadzania danych, które pozwalają zdefiniować nowy rekord. Zwróć uwagę na te trzy pola:

A. Host (*Nazwa hosta*, *Nazwa*, *Domena; Host name*, *Name*, *Domain*, itp.):

W tym polu wprowadź nazwę domeny wraz z domeną najwyższego poziomu, np:

twojafirma.com, *twojsklep.pl*, *twojeecommerce.com.pl*

B. Wartość tekstowa (*Wartość główna*, *Treść*; *Main value*, *Record*, *Content*, itp.):

W tym polu wprowadź następującą wartość:

`v=spf1 include:_spf.jupiter.salesmanago.pl`

UWAGA: Jeżeli masz już istniejący rekord `v=spf1`, wystarczy, że rozszerzysz go o następujący fragment kodu:

`include:_spf.jupiter.salesmanago.pl`

Przykładowo, jeżeli aktualny wpis to:

`v=spf1 mx include: _spf.google.com -all`

Zmień go na:

`v=spf1 mx include: _spf.google.com`
`include:_spf.jupiter.salesmanago.pl` `-all`

Zauważ, że flagi, takie jak `-all`, powinny być umieszczone po nowo dodanym fragmencie wpisu.

C. TTL (Time to Live – czas życia):
Czas TTL (Time to Live) powinien być ustawiony na 1 godzinę (3600 sekund).

Kliknij *Zapisz*, *OK*, *Gotowe*, itp., aby dodać gotowy rekord. Nie musisz podejmować żadnych dodatkowych kroków na platformie SALESmanago.

WAŻNE: Protokół SPF zostanie wdrożony dla twojej domeny w ciągu kilku godzin, ale **mogą minąć nawet 24 godziny, zanim zmiany będą widoczne w ustawieniach twojej domeny** (opóźnienie spowodowane propagacją DNS).

Krok 3.2. Dodawanie protokołu DKIM

Dodaj **dwa rekordy CNAME** dla twojej domeny. Prawdopodobnie zobaczysz kilka pól wprowadzania danych, które pozwolą ci zdefiniować nowy rekord. Zwróć uwagę na pola opisane poniżej.

REKORD CNAME 1:

A. Host (*Nazwa hosta*, *Nazwa*, *Domena; Host name*, *Name*, *Domain*, itp.):

W tym polu wprowadź następującą wartość:

```
salesmanago._domainkey.example.com
```

zastępując fragment podświetlony na zielono własną domeną.

PRZYKŁADY:

`salesmanago._domainkey.`*twojafirma.com*
`salesmanago._domainkey.`*twojsklep.pl*
`salesmanago._domainkey.`*twojeecommerce.com.pl*

B. Wartość tekstowa (*Wartość główna*, *Treść*; *Main value*, *Record*, *Content*, itp.):

W tym polu wprowadź następującą wartość:

`salesmanago._domainkey.smgrid.com`

C. TTL (Time to Live – czas życia):

Czas TTL (Time to Live) powinien być ustawiony na 1 godzinę (3600 sekund).

Kliknij *Zapisz*, *OK*, *Gotowe*, itp., aby dodać gotowy rekord. Następnie **dodaj drugi rekord CNAME**, opisany na następnej stronie.

REKORD CNAME 2:

A. **Host (*Nazwa hosta*, *Nazwa*, *Domena; Host name*, *Name*, *Domain*, itp.):**

W tym polu wprowadź następującą wartość:

```
salesmanago2._domainkey.example.com
```

zastępując fragment podświetlony na zielono własną domeną.

PRZYKŁADY:

`salesmanago2._domainkey.`*twojafirma.com*
`salesmanago2._domainkey.`*twojsklep.pl*
`salesmanago2._domainkey.`*twojeecommerce.com.pl*

B. **Wartość tekstowa (*Wartość główna*, *Treść*; *Main value*, *Record*, *Content*, itp.):**

W tym polu wprowadź następującą wartość:

`salesmanago2._domainkey.smgrid.com`

C. **TTL (Time to Live – czas życia):**

Czas TTL (Time to Live) powinien być ustawiony na 1 godzinę (3600 sekund).

Kliknij *Zapisz*, *OK*, *Gotowe*, itp., aby dodać gotowy rekord.

WAŻNE: Protokół DKIM zostanie wdrożony dla twojej domeny w ciągu kilku godzin, ale **mogą minąć nawet 24 godziny, zanim zmiany będą widoczne w ustawieniach twojej domeny** (opóźnienie spowodowane propagacją DNS).

WAŻNE: Na tym etapie twoja konfiguracja DKIM musi zostać sprawdzona przez SALESmanago w celu potwierdzenia własności twojej domeny. Wymóg ten ma na celu zwiększenie bezpieczeństwa twojego konta i twoich e-maili oraz ochronę Klientów przed phishingiem.

Możesz umożliwić SALESmanago automatyczną weryfikację własności twojej domeny poprzez dodanie kolejnego rekordu TXT do twoich ustawień DNS (zob. Krok 3.3). W ten sposób unikniesz kontaktowania się z naszym działem Supportu, dzięki czemu zaoszczędzisz czas.

Krok 3.3. Automatyzacja weryfikacji protokołu DKIM przez SALESmanago poprzez dodanie specjalnego rekordu TXT (opcjonalne)

Po wdrożeniu protokołu DKIM (poprzez dodanie dwóch rekordów CNAME opisanych powyżej), własność twojej domeny musi zostać zweryfikowana przez SALESmanago. Wymóg ten ma na celu zwiększenie bezpieczeństwa twojego konta i twoich e-maili, a także ochronę klientów SALESmanago przed phishingiem.

Własność twojej domeny może zostać potwierdzona automatycznie, jeżeli w ustawieniach DNS twojej domeny dodasz kolejny rekord TXT. Jest to opcja zalecana, ponieważ przyspieszy to proces weryfikacji, pozwalając ci zaoszczędzić czas.

W innym wypadku, gdy tylko wdrożysz protokół DKIM, prosimy o kontakt pod adresem: support@salesmanago.com i zgłoszenie konieczności zweryfikowania własności domeny przez naszych specjalistów.

Jeżeli chcesz skorzystać z opcji zautomatyzowanej, **dodaj kolejny rekord TXT dla twojej domeny** i wypełnij jego pola w następujący sposób:

A. **Host (*Nazwa hosta*, *Nazwa*, *Domena; Host name*, *Name*, *Domain*, itp.):**

   W tym polu wprowadź nazwę domeny wraz z domeną najwyższego poziomu, np:

   twojafirma.com, *twojsklep.pl*, *twojeecommerce.com.pl*

B. **Wartość tekstowa (*Wartość główna*, *Treść*; *Main value*, *Record*, *Content*, itp.):**

   W tym polu wprowadź następującą wartość:

   `smv=IdKlienta`

   zastępując fragment podświetlony na zielono własnym ID Klienta.

   Swoje ID Klienta możesz sprawdzić na platformie SALESmanago, przechodząc do **Menu → Centrum Integracji → API → zakładka API v2**.

C. **TTL (Time to Live – czas życia):**

   Czas TTL (Time to Live) powinien być ustawiony na 1 godzinę (3600 sekund).

Kliknij *Zapisz*, *OK*, *Gotowe*, itp., aby dodać gotowy rekord. Teraz własność twojej domeny zostanie zweryfikowana przez SALESmanago automatycznie. Na tym etapie możesz przejść do konfiguracji protokołu DMARC.

Krok 3.4. Dodawanie protokołu DMARC

UWAGA: Przed wdrożeniem protokołu DMARC, upewnij się, że masz wdrożone protokoły SPF i DKIM. Prawdopodobnie możesz to sprawdzić w tym samym panelu sterowania/użytkownika/konfiguracji.

Upewnij się również, że twój protokół DKIM został zweryfikowany przez SALESmanago (w celu potwierdzenia własności twojej domeny i zwiększenia twojego bezpieczeństwa). Zalecana opcja to zautomatyzowanie weryfikacji poprzez dodanie kolejnego rekordu TXT w ustawieniach DNS (Krok 3.3).

Dodaj **rekord TXT** dla swojej domeny.

Prawdopodobnie zobaczysz kilka pól wprowadzania danych, które pozwolą ci zdefiniować nowy rekord. Zwróć uwagę na te trzy pola:

A. **Host (*Nazwa hosta*, *Nazwa*, *Domena; Host name*, *Name*, *Domain*, itp.):**

W tym polu wprowadź następującą wartość:

```
_dmarc.example.com
```

zastępując fragment podświetlony na zielono własną domeną, z której wysyłasz wiadomości.

PRZYKŁADY:

`_dmarc.twojafirma.com`

`_dmarc.twojsklep.pl`

`_dmarc.twojeecommerce.com.pl`

B. Wartość tekstowa (*Wartość główna*, *Treść*; *Main value*, *Record*, *Content*, itp.):

W tym polu wprowadź swój rekord DMARC. Jeżeli masz wątpliwości, jakich parametrów i wartości użyć w swoim rekordzie DMARC, rozważ zastosowanie formatu zalecanego przez SALESmanago.

ZALECANY FORMAT DMARC

```
v=DMARC1; p=quarantine; rua=mailto:twojadresemail@twojadomena.pl;
ruf=mailto:adreswprzypadkuniepowodzenia@twojadomena.pl; adkim=r;
aspf=r;
```

Skopiuj tę formułę i wklej ją w głównym polu nowego rekordu TXT, zastępując szczegóły podświetlone na zielono własnymi danymi:

- Parametr **rua** to adres, na który będziesz otrzymywać zbiorcze raporty dotyczące ruchu twojej komunikacji e-mail.
- **Ruf** to adres, na który będziesz otrzymywać raporty o nieudanych próbach uwierzytelnienia. Zauważ, że ten parametr nie jest obsługiwany przez Gmail.

PRZYKŁADY:

```
v=DMARC1; p=quarantine; rua=mailto:emailmanager@twojafirma.com;
ruf=mailto:emailfailures@twojafirma.com; adkim=r; aspf=r;
```

```
v=DMARC1; p=quarantine; rua=mailto:administrator@twojsklep.com.pl;
ruf=mailto:niepowodzeniadmarc@twojsklep.com.pl; adkim=r; aspf=r;
```

Możesz także dostosować poszczególne wartości na podstawie parametrów (tagów) oraz definicji przedstawionych w Dodatku do tego dokumentu.

UWAGA: Zalecamy uwzględnienie następujących tagów:: aspf=r; adkim=r; w formule rekordu. W przeciwnym razie, jeżeli ustawisz swoją politykę na cokolwiek innego niż p=none, twoje wiadomości w ogóle nie będą dostarczane.

C. **TTL (Time to Live – czas życia):**

Czas TTL (Time to Live) powinien być ustawiony na 1 godzinę (3600 sekund).

Kliknij *Zapisz*, *OK*, *Gotowe*, itp., aby dodać gotowy rekord. Nie musisz podejmować żadnych dodatkowych kroków na platformie SALESmanago.

WAŻNE: Protokół DMARC zostanie wdrożony dla twojej domeny w ciągu kilku godzin, ale **mogą minąć nawet 24 godziny, zanim zmiany będą widoczne w ustawieniach twojej domeny** (opóźnienie spowodowane propagacją DNS).

Jeżeli masz jakiekolwiek pytania lub wątpliwości dotyczące konfiguracji protokołów uwierzytelniania, bądź jeśli chcesz, aby twoja konfiguracja została zweryfikowana przez naszego specjalistę, skontaktuj się z nami pod adresem:

support@salesmanago.com

---

3. Szybkie podsumowanie

W poniższej tabeli podsumowano wpisy DNS wymagane w świetle nowych polityk Gmail oraz Yahoo. Przejrzyj jej zawartość i porównaj z twoimi nowymi rekordami.

Pamiętaj, że szczegóły zaznaczone na zielono to tylko placeholdery, które muszą zostać zastąpione twoimi własnymi danymi.

Protokół	Nazwa	Rodzaj	Wartość	TTL
SPF	example.com	TXT	v=spf1 include:_spf.jupiter.salesmanago.pl	3600
DKIM	salesmanago._domainkey.example.com	CNAME	salesmanago._domainkey.smgrid.com	3600
	salesmanago2._domainkey.example.com	CNAME	salesmanago2._domainkey.smgrid.com	3600
DMARC	_dmarc.example.com	TXT	v=DMARC1; p=quarantine; rua=mailto:dmarcreports@example.com ; ruf=mailto:dmarcreports@example.com ; adkim=r; aspf=r;	3600

UWAGA: Jeżeli masz istniejący rekord v=spf1, wystarczy, że rozszerzysz go o następujący fragment kodu:

`include:_spf.jupiter.salesmanago.pl`

Zauważ, że flagi, takie jak -all, powinny być umieszczone po nowo dodanym fragmencie wpisu. Zob. Krok 3.1.

Ponadto zachęcamy do dodania kolejnego rekordu **TXT, który umożliwi** SALESmanago automatyczną weryfikację własności twojej domeny. W ten sposób unikniesz konieczności skontaktowania się z naszym działem Supportu po wdrożeniu DKIM.
Więcej informacji znajdziesz w **Kroku 3.3**.

Rekord	Nazwa	Rodzaj	Wartość	TTL
Automatyczna weryfikacja DKIM przez SALESmanago	example.com	TXT	smv=clientId	3600

DODATEK: Elementy rekordu DMARC

W poniższej tabeli przedstawiono parametry (tagi) oraz wartości dla rekordów DMARC, tak jak zostały opisane przez Google:

https://support.google.com/a/answer/10032169?sjid=14098442164638657890-EU#zippy=%2Cdmarc-record-tag-definitions-and-values

W tabeli opisano poszczególne elementy rekordu DMARC oraz dostępne opcje konfiguracji.

Jeżeli masz wątpliwości, jakich wartości użyć dla swojego rekordu DMARC, możesz zastosować format zalecany przez SALESmanago (zob. Sekcja 3.3 powyżej).

Tag	Opis i wartości
v	Wersja DMARC. Musi to być DMARC1. **Ten tag jest wymagany.**
p	Informuje serwer poczty przychodzącej, co zrobić z wiadomościami, które nie przejdą uwierzytelniania. **none** – Względem wiadomości nie są podejmowane żadne działania i zostaje ona dostarczona do adresata. Wiadomości są zapisywane w raporcie dziennym. Raport jest wysyłany na adres e-mail określony w rekordzie za pomocą opcji rua. **quarantine** – Wiadomości są oznaczane jako spam i umieszczane w folderze spamu odbiorcy. Adresaci mogą przeglądać te wiadomości, aby sprawdzić, czy na pewno powinny trafić do spamu. **reject** – Wiadomość jest odrzucana. W przypadku tej opcji serwer odbierający zwykle wysyła do serwera wysyłającego wiadomość o problemie z dostarczeniem. **Ten tag jest wymagany.** Uwaga dotycząca BIMI: Jeśli w domenie jest używany rekord BIMI, opcja p zasad DMARC musi być ustawiona jako quarantine lub reject. BIMI nie obsługuje zasad DMARC z opcją p ustawioną jako none.

pct	Określa, jaki procent nieuwierzytelnionych wiadomości podlega zasadom DMARC. Kiedy stopniowo wdrażasz DMARC, możesz zacząć od niewielkiego procentu wiadomości. Gdy coraz więcej wiadomości z twojej domeny zacznie przechodzić uwierzytelnianie przez serwery odbierające, możesz zwiększać wartość procentową, aż osiągniesz 100%. Wartość musi być liczbą całkowitą z zakresu od 1 do 100. Jeśli nie wybierzesz tej opcji w rekordzie, zasady DMARC będą stosowane do wszystkich wiadomości wysyłanych z twojej domeny.. **Ten tag jest opcjonalny.** Uwaga dotycząca BIMI: jeśli w domenie jest używany rekord BIMI, wartość pct w zasadach DMARC musi być równa 100. BIMI nie obsługuje zasad DMARC z wartością pct mniejszą niż 100.
rua	Adres e-mail, na który są wysyłane raporty o działaniach DMARC dla twojej domeny. Adres e-mail musi zawierać ciąg znaków mailto: Przykład: mailto:dmarc-reports@solarmora.com Aby wysyłać raporty DMARC na wiele adresów e-mail, rozdziel adresy e-mail przecinkami i dodaj prefiks mailto: przed każdym adresem. Przykład: mailto:dmarc-reports@solarmora.com, mailto:dmarc-admin@solarmora.com Użycie tej opcji może powodować otrzymywanie dużej liczby e-maili z raportami. Nie zalecamy używania własnego adresu e-mail. Lepszym rozwiązaniem może być stworzenie osobnej skrzynki pocztowej albo grupy lub skorzystanie z usług innej firmy, która specjalizuje się w raportach DMARC. **Ten tag jest opcjonalny.**
ruf	Nieobsługiwane. Gmail nie obsługuje tagu ruf używanego do wysyłania raportów o niepowodzeniu. Raporty te są też nazywane raportami śledczymi.

sp	Ustawia zasady dla wiadomości z subdomen domeny podstawowej. Użyj tej opcji, jeśli w subdomenach chcesz stosować inne zasady DMARC. **none** – Względem wiadomości nie są podejmowane żadne działania i zostaje ona dostarczona do adresata. Wiadomości są zapisywane w raporcie dziennym. Raport jest wysyłany na adres e-mail określony w rekordzie za pomocą opcji rua. **quarantine** – Wiadomości są oznaczane jako spam i umieszczane w folderze spamu odbiorcy. Adresaci mogą przeglądać te wiadomości, aby sprawdzić, czy na pewno powinny trafić do spamu. **reject** – Wiadomość jest odrzucana. W takim przypadku serwer odbierający powinien wysłać do serwera wysyłającego wiadomość o problemie z dostarczeniem. Jeśli nie wybierzesz tej opcji w rekordzie, subdomeny odziedziczą zasady DMARC ustawione w domenie nadrzędnej. **Ten tag jest opcjonalny.**
adkim	Ustawia zasady dopasowania DKIM określające poziom zgodności informacji o wiadomościach z podpisami DKIM. (...) **s** – Dopasowanie ścisłe. Nazwa domeny nadawcy musi być dokładnie taka sama jak odpowiednia wartość *d=nazwadomeny* z nagłówków DKIM poczty. **r** – Dopasowanie luźne (domyślnie). Zezwala na dopasowanie częściowe. Akceptowana jest każda poprawna subdomena domeny określonej w kluczu DKIM (w parametrze *d=domain*). **Ten tag jest opcjonalny.**
aspf	Ustawia zasady dopasowania SPF określające poziom zgodności informacji o wiadomościach z podpisami SPF. (...) **s** – Dopasowanie ścisłe. Nagłówek Od: wiadomości musi być dokładnie taki sam jak nazwa domeny z polecenia SMTP MAIL FROM. **r** – Dopasowanie luźne (domyślnie). Zezwala na dopasowanie częściowe. Akceptowana jest każda poprawna subdomena wartości, która jest nazwą domeny. **Ten tag jest opcjonalny.**

Źródło: Google Help Center
https://support.google.com/a/answer/10032169?sjid=14098442164638657890-EU#zippy=%2Cdmarc-record-tag-definitions-and-values