# Häufig gestellte Fragen zur ESA: Wie konfiguriere ich die Bounce-Verifizierung für die ESA?

## Inhalt



## Einführung

In diesem Dokument wird beschrieben, wie Sie die Bounce-Verifizierung für die Cisco E-Mail Security Appliance (ESA) konfigurieren.

## Voraussetzungen

### Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Cisco ESA
- AsyncOS

### Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Hardware- und Softwareversionen:

- Cisco ESA, alle Versionen von AsyncOS

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

# Hintergrundinformationen

Dieser Abschnitt bietet eine Übersicht über das Tagging und die Bounce-Verifizierung auf der ESA.

## Übersicht über die Bounce-Verifizierung

Wenn eine E-Mail mit aktivierter Bounce-Verifizierung gesendet wird, schreibt Ihre ESA die Umschlagabsenderadresse in der Nachricht neu. Beispiel: **MAIL FROM: joe@example.com** wird **MAIL FROM: prvs=joe=123ABCDEFG@example.com**. Die **123 ...** im Beispiel ist das *Bounce-Verifizierungs-Tag*, das dem Umschlagabsender hinzugefügt wird, während es von der Appliance gesendet wird. Wenn die Nachricht abprallt, enthält die Empfängeradresse des Umschlags in der Bounce in der Regel den Bounce-Verifizierungs-Tag.

> **Hinweis**: Weitere Informationen finden Sie im Abschnitt **Adressmarkierungsschlüssel für die Konfiguration der Bounce-Verifizierung** im **erweiterten Benutzerhandbuch**.

Sie können das systemweite Tagging der Bounce-Verifizierung als Standard aktivieren oder deaktivieren. Sie können auch das Tagging der Bounce-Verifizierung für bestimmte Domänen aktivieren oder deaktivieren. In den meisten Fällen aktivieren Sie es standardmäßig, und listen Sie dann bestimmte Domänen für den Ausschluss in der Tabelle Zielsteuerelemente auf.

Wenn eine Content Security Appliance eine Bounce-Nachricht mit bereits markierter Adresse an eine andere Content Security Appliance innerhalb der De-Militarized Zone (DMZ) sendet, fügt AsyncOS kein weiteres Tag hinzu.

> **Vorsicht**: Wenn Sie die Bounce-Verifizierung aktivieren, können Ihre Appliances legitime E-Mails ablehnen, die mit einem leeren Umschlagabsender gesendet werden.

# Wie konfiguriere ich die Bounce-Verifizierung für die ESA?

Gehen Sie wie folgt vor, um die Bounce-Verifizierung für die ESA zu konfigurieren:

1. Navigieren Sie zu **Mail-Policys > Bounce-Verifizierung**, und geben Sie manuell einen Tagging-Schlüssel mit einer zufälligen Auswahl von Zahlen und Buchstaben ein, z. B. **4r5t6y7u**.

2. Einstellungen für die Bounce-Verifizierung bearbeiten:

   Navigieren Sie zu **Mail-Policys > Zielsteuerelemente**, und aktivieren Sie die Bounce-Verifizierung.

   Wählen Sie **Standard** im Feld Domain (Domäne) (oder Ihrem benutzerdefinierten Ziel) aus.

   Wenn das Fenster Default (Standard) geöffnet und der Abschnitt Bounce-Verifizierung

angezeigt wird, klicken Sie auf **Yes (Ja)**.

3. Stellen Sie sicher, dass nicht getaggte (fehlgeleitete) Bounces blockiert sind:

   Navigieren Sie zu **Mail-Policys > Mail Flow-Policys**.

   Wählen Sie die entsprechende Richtlinie aus, und suchen Sie den Abschnitt Sicherheitsfunktionen.

   Stellen Sie sicher, dass der Wert Untagged Bounces auswerten auf **No** festgelegt ist. Bei früheren Versionen von AsyncOS sollte der Wert Untagged Bounces akzeptieren auf **No** festgelegt werden.