

Wie kann ich Warnungen hinzufügen/ändern, die von der Cisco Web Security Appliance per E-Mail gesendet werden?

Inhalt

[Frage](#)

[Umgebung](#)

Frage

Wie kann ich Warnungen hinzufügen/ändern, die von der Cisco Web Security Appliance per E-Mail gesendet werden?

Umgebung

Cisco Web Security Appliance (WSA), alle Versionen von AsyncOS.

Die Cisco Web Security Appliance (WSA) verfügt über zahlreiche verschiedene E-Mail-Warnmeldungen, die versendet werden. Sie können festlegen, welche Warnmeldungen gesendet werden und an welche E-Mail-Adressen. Dies kann über die CLI oder die GUI erfolgen. Bitte beachten Sie die folgenden Anweisungen:

Benutzeroberfläche

Gehen Sie zur Registerkarte "Systemverwaltung" -> "Warnungen":

- Um die Warnungen für eine bereits konfigurierte E-Mail-Adresse zu ändern, klicken Sie auf die E-Mail-Adresse, die Sie ändern möchten.
- Um eine neue E-Mail-Adresse zum Empfang der Warnmeldungen hinzuzufügen, klicken Sie auf "Empfänger hinzufügen..". -Taste.

CLI

WSA_CLI> Warnkonfiguration

Senden von Warnmeldungen an:

admin@domain.com

Klasse: Alle - Schweregrade: Alle

Anfängliche Wartezeit in Sekunden, bevor eine doppelte Warnmeldung gesendet wird: 300
Maximale Wartezeit in Sekunden, bis ein Alert-Doppel gesendet wird: 3600

Warnungen werden mit der Standardeinstellung "From Address" (Von Adresse) gesendet.

.....

Wählen Sie den Vorgang aus, den Sie ausführen möchten:

- NEU - Fügen Sie eine neue E-Mail-Adresse hinzu, um Warnungen zu senden.
- BEARBEITEN - Ändern Sie das Warnabonnement für eine E-Mail-Adresse.
- LÖSCHEN - Entfernen Sie eine E-Mail-Adresse.
- Löschen - Entfernen Sie alle E-Mail-Adressen (Warnmeldungen deaktivieren).
- SETUP - Konfigurieren der Alarmeinstellungen
- FROM - Konfigurieren der Von-Adresse von Alert-E-Mails.

[]> neu

Geben Sie eine neue E-Mail-Adresse ein, um Warnungen zu senden (z. B.:

["administrator@example.com"](mailto:administrator@example.com))

[]> email@test.com

Wählen Sie die Alert-Klassen aus. Trennen Sie mehrere Auswahlmöglichkeiten durch Kommas.

1. Alle
2. System
3. Hardware
4. Updater
5. Webproxy
6. DVS und Anti-Malware
7. L4-Datenverkehrsüberwachung

[1]> 2,4,7

Wählen Sie einen Schweregrad aus. Trennen Sie mehrere Auswahlmöglichkeiten durch Kommas.

1. Alle
2. Kritisch
3. Warnung
4. Informationen

[1]> 1

Hinweis:

Sie können mehrere Warnklassen und Schweregrade auswählen, indem Sie die entsprechenden Nummern durch ein Komma trennen.

Beispiel:

Im vorherigen Beispiel (2,4,7) lauten die zu sendenden Warnungen 'System', 'Updater' und 'L4 Traffic Monitor'.

Möglicherweise möchten Sie nicht, dass alle ausgewählten Alert-Klassen den gleichen Schweregrad haben. In diesem Fall müssen Sie nach Angabe des Schweregrads die Option "Edit" (Bearbeiten) auswählen und jeden Schweregrad pro Alert-Klasse angeben.