Endbenutzerhandbuch

TRITON AP-EMAIL Cloud

10900 Stonelake Blvd, 3rd Floor, Austin, TX 78759, USA

Veröffentlicht 2015
Gedruckt in den Vereinigten Staaten von Amerika und China.

Warenzeichen

Inhalt

1 TRITON AP-EMAIL verwenden

Einführung

Willkommen zum *Benutzerhandbuch für TRITON AP-EMAIL*. Ihre Organisation hat sich für den von Websense angebotenen Dienst TRITON AP-EMAIL angemeldet.

Dieses Handbuch beschreibt, wie der Dienst funktioniert und erläutert, wie Sie Ihre E-Mails kontrollieren und die Menge unerwünschter E-Mails, sogenannter Spam-E-Mails, reduzieren können.

Was ist Websense TRITON AP-EMAIL?

Websense TRITON AP-EMAIL ist ein Dienst, der all Ihre ein- und abgehenden Internet-E-Mails (d.h. E-Mails, die sich außerhalb der internen Domäne Ihres Unternehmens befinden) filtert. Der Dienst durchsucht eingehende E-Mails, bevor diese Ihr Netzwerk erreichen, und filtert unerwünschte Nachrichten auf Basis einer von Ihrem E-Mail-Administrator definierten Richtlinie heraus.

TRITON AP-EMAIL wird normalerweise verwendet, um E-Mails herauszufiltern, die Viren und Spam enthalten. Der Dienst kann jedoch auch verwendet werden, um andere Arten von Inhalten zu blockieren, beispielsweise Nachrichten mit angehängten Filmen oder ausführbaren Dateien, oder Nachrichten, die obszöne oder unangemessene Wörter oder Ausdrücke enthalten.

Wie wirkt sich der Dienst auf mich aus?

Im Allgemeinen werden Sie kaum bemerken, dass Websense TRITON AP-EMAIL eingesetzt wird. Ihre E-Mails werden normal ausgeliefert, aber Sie werden wahrscheinlich feststellen, dass die Menge an unerwünschten „Junk-E-Mails“, die Sie erhalten, nachlässt.

TRITON AP-EMAIL kann auf zwei Arten mit Ihnen kommunizieren:

1. **Benachrichtigungs-E-Mail**: Es kann vorkommen, dass Sie von Zeit zu Zeit darüber informiert werden, dass eine Nachricht blockiert wurde. Dies kommt normalerweise nur dann vor, wenn jemand versucht hat, Ihnen eine E-Mail-Nachricht zu senden, die einen Virus oder andere unzulässige Inhalte enthält. In der Benachrichtigung erhalten Sie einen Link, auf den Sie klicken können, um weitere Informationen über die blockierte Nachricht zu erhalten.
2. **Nachrichtenbericht für Endbenutzer:** TRITON AP-EMAIL kann Ihnen in regelmäßigen Abständen einen Nachrichtenbericht zusenden. Dieser enthält Informationen über alle E-Mails, die Sie erhalten und gesendet haben, und bietet Ihnen die Möglichkeit, Aktionen für Nachrichten durchzuführen, die als Spam behandelt wurden. Unter *Woher weiß ich, welche Nachrichten blockiert wurden?*, Seite 3 erhalten Sie weitere detaillierte Informationen hierzu.

Wirkt sich TRITON AP-EMAIL auf diejenigen aus, die mir E-Mails schicken?

Nein. Der Dienst schickt keine Benachrichtigungen an Absender, wenn deren eingehenden E-Mails einen Virus enthalten und blockiert wurden.

Wie geht TRITON AP-EMAIL mit Spam um?

Alle Nachrichten, die durch TRITON AP-EMAIL geleitet werden, werden analysiert und mit einem Spamwert versehen. Je höher dieser Wert ist, desto wahrscheinlicher ist es, dass es sich bei der Nachricht um Spam handelt. Ihr Unternehmen hat einen Spam-Grenzwert eingerichtet, und alle Nachrichten, deren Wert über dieser Grenze liegen, werden als Spam behandelt.

Nachrichten, die als Spam klassifiziert wurden, werden normalerweise in Quarantäne gestellt und 30 Tage lang gespeichert. Nachrichten mit hohen Spamwerten können unter der Kontrolle des Administrators auch entsorgt werden. Sie werden **NICHT** benachrichtigt, wenn Sie Spam erhalten. In manchen Organisationen stellt Spam 98 Prozent der eingehenden E-Mails dar. Es wäre wenig zweckdienlich, Sie über jede empfangene Spam-E-Mail zu informieren.

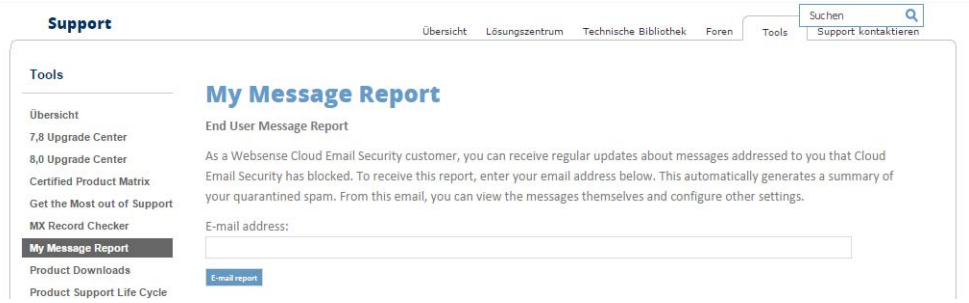
Es ist möglich, TRITON AP-EMAIL so einzurichten, dass es Spam-E-Mails mit einer Markierung versieht. Dies bedeutet, dass Spam zwar normal ausgeliefert wird, das Wort „SPAM:“ jedoch zur Betreffzeile hinzugefügt wird. Diese Funktion wird von E-Mail-Administratoren am Häufigsten zur Verwendung während einer einführenden Bewertungsphase eingerichtet oder um E-Mails zu kennzeichnen, deren Spamwert im Grenzbereich liegt.

Woher weiß ich, welche Nachrichten blockiert wurden?

TRITON AP-EMAIL kann einen Nachrichtenbericht bereitstellen, in dem alle Nachrichten aufgeführt werden, die für Ihre E-Mail-Adresse verarbeitet wurden. Dieser Bericht umfasst auch alle blockierten Nachrichten.

Besuchen Sie die folgende Webseite, um den Bericht zu erhalten:

http://www.websense.com/content/messagereport.aspx



Geben Sie Ihre E-Mail-Adresse in das bereitgestellte Feld ein. Der Bericht wird Ihnen anschließend per E-Mail zugeschickt. Normalerweise dauert dies nur einige wenige Minuten und hängt von der entsprechenden Datenmenge ab.

Was ist im Nachrichtenbericht enthalten?

Der Nachrichtenbericht enthält zahlreiche nützliche Informationen. Das nachfolgende Beispiel zeigt die Online-Version des Berichts, auf den Sie durch einen Klick auf den Link **Berichte anzeigen** in der E-Mail-Version zugreifen können.

	Inhalt
A	Der Zeitraum, für den der Bericht erstellt wurde
B	Ihre E-Mailadresse
C	Die Anzahl verdächtiger und sauberer Nachrichten, die während des Zeitraums für Sie verarbeitet wurden
D	Eine Option, um die Anzahl der im Bericht angezeigten Tage zu ändern
E	Ein Link, über den Sie angeben können, dass Sie diesen Bericht regelmäßig per E-Mail erhalten möchten
F	Die Möglichkeit, alle in Quarantäne gestellten und/oder Spam-Nachrichten auszuwählen und Aktionen für diese durchzuführen, beispielsweise um diese zu löschen oder freizugeben
G	Ein Link, über den Sie Ihre Subskription für den Bericht ändern können
H	Ein Link, über den Sie Ihre persönlichen Positiv- und Negativlisten verwalten können

	Inhalt
I	Eine Liste Ihrer E-Mails in der folgenden Reihenfolge (Liste hängt von der Konfiguration für den Benutzer und das Konto ab): • Verdächtige Nachrichten, die Sie erhalten oder versandt habe • Saubere Nachrichten, die Sie erhalten oder versandt habe Wenn Sie die Online-Version Ihres Berichts betrachten, können Sie die Reihenfolge der Nachrichten ändern, indem Sie auf einen Link in der Kopfzeile einer Spalte klicken. Sie können die Sortierung beispielsweise über die Spalte **Von** oder **An**, die Spalte **Datum/Uhrzeit** oder die Spalte **Status** vornehmen.
J	Ein Indikator, ob eine Nachricht empfangen oder versandt wurde. ⟵ Empfangen ⟶ Versandt
K	Die Aktionen, die Sie für eine Nachricht durchführen können. (Wählen Sie eine Nachricht aus, indem Sie auf der linken Seite auf das Markierungsfeld klicken.) Die folgenden Optionen sind verfügbar: • **Details** - Auf Detailinformationen über die Nachricht zugreifen • **Freigeben** - Die Nachricht aus der Quarantänezone freigeben. (Dies ist nicht für alle Nachrichten möglich. Wenn eine Nachricht beispielsweise Viren enthält, kann sie nicht freigegeben werden.) • **Zu Positivliste hinzufügen** - Diese E-Mail-Adresse oder Domäne zu Ihrer persönlichen Positivliste hinzufügen. Hierdurch wird der gehostete Dienst angewiesen, Nachrichten von diesem Absender bzw. von dieser Domäne zuzulassen, sofern sie keinen Virus oder Malware enthalten. • **Zu Negativliste hinzufügen** - Diese E-Mail-Adresse oder Domäne zu Ihrer persönlichen Negativliste hinzufügen. Hierdurch wird der gehostete Dienst angewiesen, Nachrichten von diesem Absender bzw. von dieser Domäne niemals zuzulassen.

Der Abschnitt mit der Nachrichtenzusammenfassung enthält die folgenden Informationen:

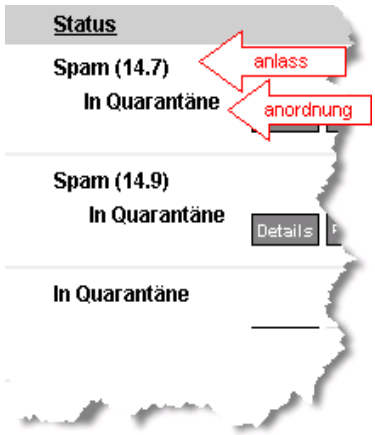
- Angabe, ob die Nachricht empfangen oder versandt wurde
- Absender der Nachricht
- Empfänger der Nachricht
- Datum und Uhrzeit, zu der TRITON AP-EMAIL die E-Mail protokolliert hat
- Status der E-Mail. Dieser enthält einen Grund und eine Disposition. (Weitere Informationen hierzu erhalten Sie unter *Was bedeutet der Status?*, Seite 5.)
- Betreffzeile der Nachricht

Was bedeutet der Status?

Die Spalte **Status** des Nachrichtenberichts für Endbenutzer enthält einen Grund (z.B. Spam) und eine Disposition (z.B. in Quarantäne gestellt).

Wenn die Nachricht nicht ausgeliefert wurde, weist das erste (fett gedruckte) Wort in dieser Spalte auf den Grund hierfür hin. Das darunter stehende Wort weist auf die

Aktion hin, die für die Nachricht vorgenommen wurde. Dies wird auch als die Disposition der Nachricht bezeichnet.



In Quarantäne gestellte Spam-Nachrichten enthalten den Spamwert. Je höher dieser Wert ist, desto wahrscheinlicher ist es, dass es sich bei der Nachricht um Spam handelt.

Die folgende Tabelle erläutert die möglichen Gründe, die Ihnen angezeigt werden können:

Begründung	Erklärung
Zugangskontrolle	Die Nachricht wurde aufgrund einer von Ihrem Administrator eingerichteten Zugangskontrollrichtlinie blockiert.
Zugangsregel	Die Nachricht wurde aufgrund einer von Ihrem Administrator eingerichteten Zugangskontrollrichtlinie blockiert.
Anhang blockiert	Die Nachricht enthält einen Anhang, dessen Typ von Ihrer Richtlinie blockiert wurde.
Blockierte ausführbare Datei	Die Nachricht enthält einen ausführbaren Anhang, und ausführbare Dateien werden von Ihrer Richtlinie blockiert.
In Negativliste	Die E-Mail-Adresse oder Domäne dieses Absenders befindet sich in Ihrer persönlichen Negativliste oder in der Negativliste Ihrer Richtlinie.
Sauber	Die Nachricht verstößt gegen keine Ihrer eingerichteten Richtlinien.

Begründung	Erklärung
Gefährlicher Inhalt	Die Nachricht enthält Inhalte, die für Ihre Maschine gefährlich sein könnten. Hierfür kann es mehrere untergeordnete Gründe geben: **Datei mit doppelter Dateierweiterung** - Der Dateiname eines Anhangs hat eine doppelte Dateierweiterung, was zur Maskierung der echten Funktion der Datei verwendet werden kann. **Leeres Archiv** - Die Nachricht enthält eine leere Archivdatei. **Ausführbare Datei in Service-Nachricht** - Bei der Nachricht handelt es sich um eine Meldung zum Auslieferungsstatus, die ausführbaren Inhalt enthält. **openrelay(block)** - Der Absender der Nachricht hätte nicht in der Lage sein sollen, E-Mails über den abgehenden E-Mail-Server zu senden. **Gespoofter Virus** - Die Nachricht enthält einen Virus. Der Absender der Nachricht scheint gefälscht zu sein. **Verdächtige Anhänge** - ThreatSeeker hat einen verdächtigen Anhang $1 in der Nachricht gefunden. **Archiv mit null Byte** - Die Nachricht enthält einen leeren Archivdateianhang. Dies liegt wahrscheinlich daran, dass ein Virus entfernt wurde. **Ausführbare Datei mit null Byte** - Die Nachricht enthält einen leeren Anhang für eine ausführbare Datei. Dies liegt wahrscheinlich daran, dass ein Virus entfernt wurde.
Erweiterung maskiert	Die Nachricht enthält einen Anhang, dessen Erweiterung gemäß der Konfiguration Ihrer Richtlinie umbenannt wurde. Eine Erweiterung für ausführbare Dateien kann beispielsweise in „.ex_“ umbenannt werden, um eine Ausführung zu verhindern.

Begründung	Erklärung
Format	Für den Grund Format kann es mehrere untergeordnete Gründe geben: • **Extraktion eines Archivs fehlgeschlagen** - Der Dienst war nicht in der Lage, eine Archivdatei zu entpacken, und konnte diese nicht scannen. • **Anhang ohne Dateiname** - Ein Anhang der Nachricht hat keinen angegebenen Dateinamen. Dies kann verwendet werden, um bestimmte E-Mail-Clients anzugreifen. • **E-Mail nicht mehrteilig** - Die Struktur der Nachricht ist möglicherweise schädlich und kann verwendet werden, um bestimmte E-Mail-Clients anzugreifen. • **Verschlüsselt** - Die Nachricht oder ein Anhang ist verschlüsselt. • **Erweiterungsstufe überschritten** - Die Nachricht enthielt zu viele Ebenen verschachtelter Archive. Die Archivinhalte konnten nicht gescannt werden. • **Dateiname blockiert** - Der Name des Anhangs stimmt mit einer vom Dienst konfigurierten Regel überein. • **Dateiname zu lang** - Die Betreffzeile enthält einen Dateinamen, der zu lang ist. Dies kann verwendet werden, um bestimmte E-Mail-Clients anzugreifen. • **Kopfzeile blockiert** - Die Kopfzeile der Nachricht verstößt gegen eine Regel der konfigurierten Richtlinie. • **Kopfzeile enthält große Datenblöcke** - Die Kopfzeile der Nachricht enthält einen Datenblock, dessen Länge über dem zulässigen Maximalwert liegt. • **Kopfzeilenlänge überschritten** - Die Länge der Kopfzeile der Nachricht überschreitet den zulässigen Maximalwert. Dies kann verwendet werden, um bestimmte E-Mail-Clients anzugreifen. • **Betreff der Nachricht blockiert** - Der Betreff der Nachricht stimmt mit einer vom Dienst konfigurierten Regel überein. • **MIME-Typ blockiert** - Die Nachricht enthält einen Anhang, der von der konfigurierten Richtlinie blockiert wird. • **Partieller Hauptteil der Nachricht** - Die Nachricht kann nicht gescannt werden, da Teile eines Anhangs fehlen, und wurde blockiert. • **Passwortgeschütztes Archiv** - Die Nachricht enthält eine passwortgeschützte Archivdatei. Diese kann nicht gescannt werden und wurde daher blockiert. • **Potenzieller Angriff auf Outlook** - Das Datum oder der Betreff der Nachricht ist zu lang. Diese können verwendet werden, um E-Mail-Clients wie beispielsweise alte Versionen von MS Outlook anzugreifen. • **Signiert** - Die Signatur der Nachricht ist verschlüsselt. Diese Nachricht kann nicht gescannt werden und wurde in Quarantäne gestellt. • **Verdächtige Zeichen im Hauptteil** - Der Hauptteil der Nachricht enthält Binärinformationen an einer unerwarteten Stelle. Dies könnte schädlich sein. • **Verdächtige Zeichen in der Kopfzeile** - Die Kopfzeile der Nachricht enthält Binärinformationen an einer unerwarteten Stelle. Dies könnte schädlich sein. • **Unzustellbarer Empfänger** - Die E-Mail-Richtlinie blockiert die Auslieferung von E-Mails an diese Subdomäne. • **Unzustellbarer Absender** - Die E-Mail-Richtlinie blockiert die Auslieferung von E-Mails von Benutzern in dieser Subdomäne.

Begründung	Erklärung
Zustellbarkeit wird ermittelt	Die Nachricht sieht verdächtig aus. Wir halten sie zurück, bis wir bestimmen können, ob sie schädlich ist.
Lexikalische Regel	Die Nachricht enthält Inhalte, die gegen eine in Ihrer Richtlinie eingerichtete lexikalische Regel verstößt.
Makro	Die Nachricht enthält vermutlich einen Makrovirus.
Nachrichtenschleife	Der Dienst hat eine Nachrichtenlieferschleife festgestellt.
Operativ	Die Nachricht wurde aus operativen Gründen blockiert.
Potenzieller Virus	Die Nachricht enthält einen potenziellen Virus, der für Ihre Maschine schädlich sein könnte.
Spam (n)	Die Nachricht wurde von Ihrer E-Mail-Richtlinie als Spam eingestuft. In Quarantäne gestellte Spam-Nachrichten enthalten einen Spamwert. Je höher dieser Wert ist, desto wahrscheinlicher ist es, dass es sich bei der Nachricht um Spam handelt.
System	Die Nachricht konnte aus Systemgründen nicht verarbeitet werden.
TempFehler	Der E-Mail-Server ist außer Betrieb und konnte vorübergehend keine E-Mails empfangen.
Zu groß	Die Größe dieser Nachricht übersteigt die in der Richtlinie angegebene Maximalgröße.
Unbekannt	Mit der Nachricht ist ein unbekanntes Problem aufgetreten.
Virus	Die Nachricht enthält einen bekannten Virus, der für Ihre Maschine schädlich ist.
In Positivliste	Die E-Mail-Adresse oder Domäne dieses Absenders befindet sich in Ihrer persönlichen Positivliste oder in der Positivliste Ihrer Richtlinie.

Die folgende Tabelle führt die möglichen Dispositionen auf:

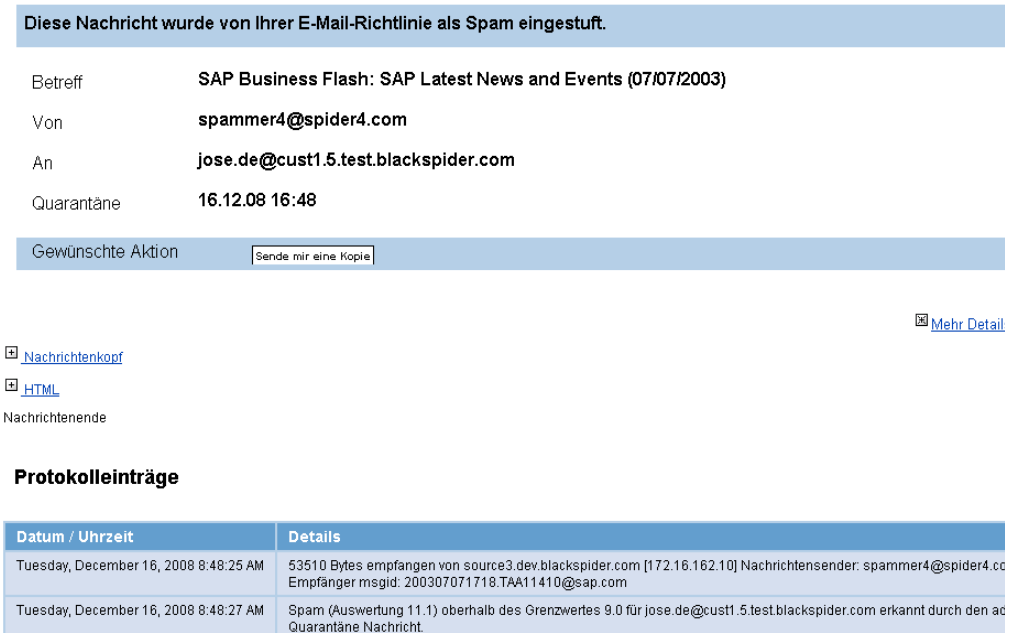
Disposition	Erklärung
Angenommen	Die Nachricht wurde angenommen und zugestellt.
Bcc	Eine nicht sichtbare Kopie der Nachricht wurde versandt, d.h. der Name des Empfängers wurde unkenntlich gemacht.
Bcc, Betreff mit Markierung versehen	Eine nicht sichtbare Kopie der Nachricht wurde versandt, die Betreffzeile wurde mit einer Markierung versehen.
Zurückgekommen	Die Nachricht war unzustellbar und wurde an den Absender zurückgeschickt.
Umgehung	Die Nachricht hat das E-Mail-Sicherheitssystem umgangen.
Entsorgt	Die Nachricht wurde aus dem Archiv gelöscht.
In Quarantäne gestellt	Die Nachricht wird in der E-Mail-Quarantänezone aufbewahrt.
Spam weitergeleitet	Diese Spam-Nachricht wurde an einen Empfänger weitergeleitet.

Disposition	Erklärung
Betreff mit Markierung versehen	Die Betreffzeile der Nachricht wurde mit einer Markierung versehen.
Temp. Fehler	Der E-Mail-Server ist außer Betrieb und konnte vorübergehend keine E-Mails empfangen.
Unbekannt	Die durchgeführte Aktion ist nicht bekannt.
Ungültig	Es wurde keine Aktion vorgenommen.

Wenn Sie eine Nachricht benötigen, die aufgrund Ihrer Richtlinienvorgaben blockiert oder in Quarantäne gestellt wurde, setzen Sie sich bitte mit Ihrem E-Mail-Administrator in Verbindung.

Wie greife ich auf meine E-Mails zu?

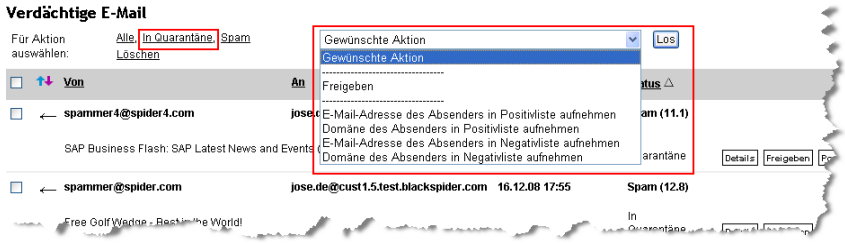
In Ihrem Nachrichtenbericht sehen Sie auf einen Blick alle Nachrichten, die Ihnen von außerhalb Ihres Netzwerks zugeschickt wurden. Der Bericht umfasst auch Nachrichten, die als Spam eingeordnet wurden, sowie all diejenigen, die aus anderen Gründen in Quarantäne gestellt wurden. Wenn Sie den Inhalt einer Nachricht anzeigen möchten, wählen Sie die Nachricht aus (indem Sie das Markierungsfeld auf der linken Seite anklicken), und klicken Sie anschließend auf **Details**. Die Detailinformationen einer Nachricht dürften in etwa folgendermaßen aussehen:



In diesem Beispiel wurde eine Nachricht in Quarantäne gestellt, weil sie von der Richtlinie als Spam klassifiziert wurde. Der Administrator hat Ihnen die Möglichkeit eingeräumt, eine Kopie der Nachricht an sich selbst zu schicken. Wenn diese Funktion

vom Administrator nicht aktiviert wurde, wird die entsprechende Schaltfläche nicht angezeigt. In manchen Fällen haben Sie auch die Möglichkeit, eine Nachricht zu Ihrer Positiv- oder Negativliste hinzuzufügen oder die Nachricht freizugeben. Wenn die E-Mail jedoch in Quarantäne gestellt wurde, weil sie einen Virus oder anstößige Wörter enthält, werden Sie unabhängig von der Konfiguration des Dienstes durch den Administrator nicht in der Lage sein, eine Kopie freizugeben.

Sie können eine Aktion für all Ihre in Quarantäne gestellten Nachrichten auf einmal durchführen, indem Sie in Ihrem Nachrichtenbericht unter **Für Aktion auswählen** auf **In Quarantäne** klicken und dann eine Aktion auswählen, die durchgeführt werden soll. Sie können Nachrichten aus der Quarantänezone freigeben oder die Adressen oder Domänen, von denen die Nachrichten versandt wurden, zur Positiv- oder Negativliste hinzufügen.



Sie können Aktionen für einzelne Nachrichten durchführen, indem Sie die jeweiligen Markierungsfelder auswählen und anschließend eine Aktionsschaltfläche wie **In Positivliste aufnehmen** oder **In Negativliste aufnehmen** auswählen.

Bewahrt TRITON AP-EMAIL eine Kopie meiner E-Mails auf?

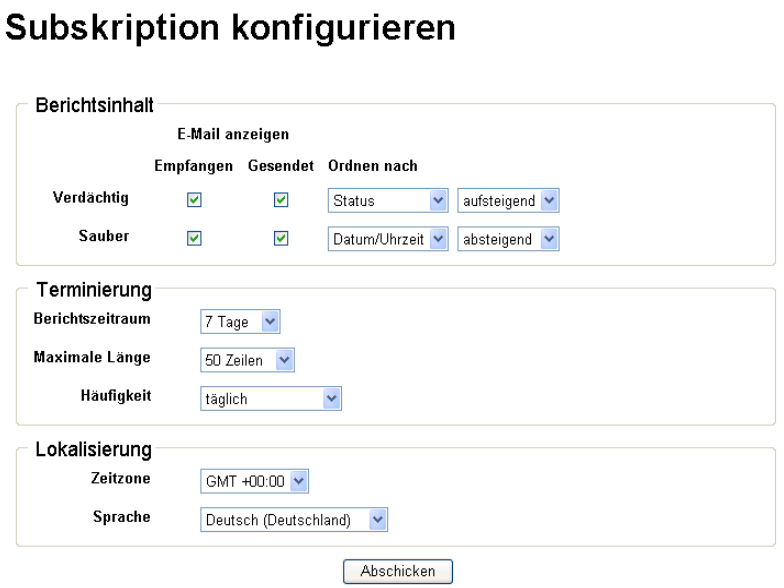
TRITON AP-EMAIL bewahrt standardmäßig keine Kopien von Nachrichten auf, sofern sie nicht in Quarantäne gestellt sind. Ihr E-Mail-Administrator kann Ihr System jedoch anderweitig konfigurieren. In Quarantäne gestellte Nachrichten werden automatisch nach 30 Tagen gelöscht. Ihr Administrator kann diese bei Bedarf jedoch auch jederzeit vorher löschen.

Wenn Sie im Nachrichtenbericht auf einen Link für eine saubere Nachricht klicken, werden nur die E-Mail-Protokolleinträge angezeigt, da die Nachricht TRITON AP-EMAIL nicht mehr zur Verfügung steht.

Kann mir TRITON AP-EMAIL den Nachrichtenbericht automatisch zusenden?

Sie können TRITON AP-EMAIL so konfigurieren, dass Ihnen die Nachrichtenberichte in einem von Ihnen bestimmten Zeitabstand zugeschickt werden. Sie können die Subskriptionsdetails definieren, indem Sie einen Bericht anfordern und

dann im Bericht auf den Link **Subskription ändern** klicken. Daraufhin wird ein Bildschirm angezeigt, der in etwa dem folgenden entspricht:



Sie können die folgenden Subskriptionsoptionen angeben:

- Berichtsinhalt
  - Welche Abschnitte sollen im Bericht enthalten sein: empfangene oder gesendete verdächtige Nachrichten, empfangene oder gesendete saubere Nachrichten?
  - In welcher Reihenfolge sollen die Informationen angezeigt werden: Nach Datum/Uhrzeit, Betreff, Absender, Empfänger, Status? In auf- oder absteigender Reihenfolge?
- Terminierung
  - Für welchen Zeitraum soll der Bericht erstellt werden: die letzten 1, 2, 7, 14 oder 30 Tage?
  - Wie viele Zeilen soll eine Seite des Berichts enthalten: 20, 50, 100, 200 oder 500?
  - Wie häufig soll der Bericht ausgeliefert werden: täglich, an Wochentagen, wöchentlich, alle zwei Wochen, monatlich oder niemals?

Hinweis

Subskriptionen für den TRITON AP-EMAIL-Nachrichtenbericht verfallen nach 90 Tagen. 62 Tage nachdem Sie sich angemeldet haben werden Sie bei jedem Erhalt eines Berichts daran erinnert, dass Sie Ihre Subskription verlängern sollten.

- Lokalisierung
  - Welche Zeitzone soll der Bericht zugrunde legen?

- In welcher Sprache soll der Bericht ausgeliefert werden? TRITON AP-EMAIL unterstützt 14 Sprachen:
  - Tschechisch
  - Niederländisch
  - Englisch
  - Französisch
  - Deutsch
  - Griechisch
  - Italienisch
  - Polnisch
  - Portugiesisch (Brasilien)
  - Portugiesisch
  - Rumänisch
  - Slowakisch
  - Spanisch
  - Schwedisch

Wie kann ich die Zusendung des Berichts abbestellen?

Sie können die Subskription Ihres Nachrichtenberichts jederzeit stornieren. Klicken Sie hierfür in einem beliebigen Bericht auf **Subskription ändern.** Wählen Sie im Bildschirm zur Konfiguration der Subskription unter **Terminierung** im Drop-Down-Feld **Häufigkeit** die Option **Niemals** aus, und klicken Sie anschließend auf **Anwenden**.

Unabhängig von den Einstellungen für die regelmäßige Zusendung des Berichts können Sie auch jederzeit einen Bericht anfordern, indem Sie das Berichtsanforderungs formular unter http://www.websense.com/content/messagereport.aspx ausfüllen.

Kann ich die Einstellungen meines Nachrichtenberichts ändern?

Sie können die Details Ihrer Subskription des Nachrichtenberichts jederzeit ändern. Klicken Sie hierfür in einem beliebigen Bericht auf **Subskription ändern.** Über denselben Bildschirm, über den Sie sich für die Zusendung des Berichts angemeldet haben, können Sie auch die Optionen für die Zusendung Ihren Wünschen entsprechend ändern.

Wie erkennt TRITON AP-EMAIL Spam?

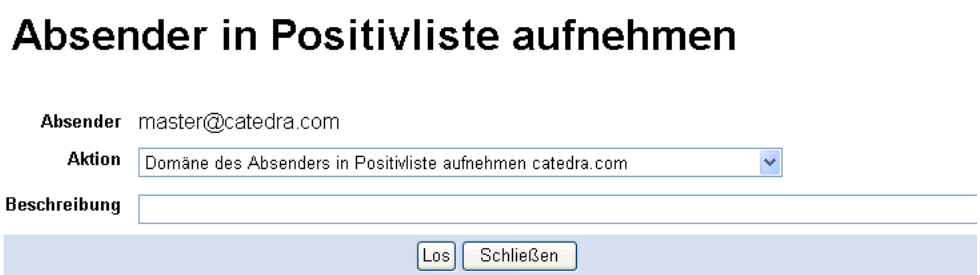
TRITON AP-EMAIL verwendet einen ausgereiften Mechanismus zur Erkennung von Spam, der regelmäßig aktualisiert wird, um neue Arten von Junk-E-Mails zu identifizieren. Da sich Spam ständig weiterentwickelt, verwendet TRITON AP-EMAIL einen adaptiven Mechanismus, der aus Erfahrungen und den Kommentaren und Rückmeldungen von Endbenutzern lernt. Darüber hinaus beschäftigen wir Spam-Analysten, die fragwürdige E-Mails prüfen und die Erkennungsmechanismen bei Bedarf aktualisieren.

Wie verhindere ich, dass TRITON AP-EMAIL gewünschte Nachrichten blockiert?

Die Definition von Spam ist subjektiv. Was für den einen Benutzer Spam ist, kann für den anderen eine legitime E-Mail darstellen. Daher kann es vorkommen, dass TRITON AP-EMAIL gelegentlich E-Mails blockiert, die Sie empfangen möchten. Normalerweise ist dies bei einem Newsletter oder bei Massen-E-Mails der Fall, die zahlreiche Eigenschaften von Spam aufweisen.

Um zu verhindern, dass TRITON AP-EMAIL diese Nachrichten in der Zukunft blockiert, können Sie den Absender zu Ihrer persönlichen Positivliste hinzufügen (sofern Ihnen Ihr Administrator hierzu die Berechtigung gegeben hat). E-Mails, die von Absendern in Ihrer Positivliste stammen, werden niemals als Spam klassifiziert. Sie können einen Absender zu Ihrer Positivliste hinzufügen, indem Sie die E-Mail im Nachrichtenbericht suchen, die Nachricht durch einen Klick in das Markierungsfeld auswählen und auf die Schaltfläche **Positivliste** klicken.

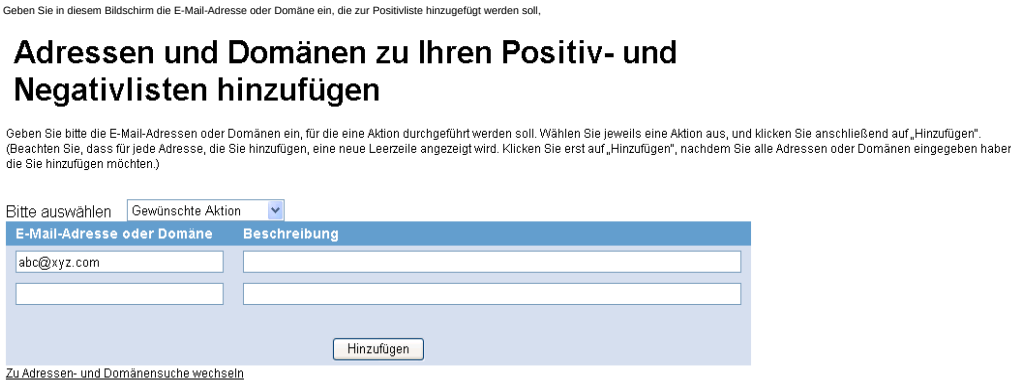
Verwenden Sie im Bildschirm, der darauf angezeigt wird, die Drop-Down-Liste, um eine Aktion vorzunehmen: **E-Mail-Adresse des Absenders in Positivliste aufnehmen** oder **Domäne des Absenders in Positivliste aufnehmen**. Klicken Sie anschließend auf **Los**.



Sie können Ihre gesamte Positivliste anzeigen oder verwalten, indem Sie in Ihrem Nachrichtenbericht **Positiv-/Negativlisten verwalten** auswählen.

Im Bildschirm, der daraufhin angezeigt wird, können Sie Ihre Positivliste auf E-Mail-Adressen oder Domänen durchsuchen. Klicken Sie auf **Positivliste anzeigen,** geben Sie Suchkriterien ein, beispielsweise die Adresse, die Sie finden möchten, und klicken Sie anschließend auf **Suchen**. Sie können angeben, wie die Ergebnisse sortiert werden sollen und wie viele Ergebnisse angezeigt werden sollen.

Wenn Sie eine Adresse zu Ihrer Positivliste hinzufügen möchten, die noch nicht darin enthalten ist, klicken Sie auf den Link Klicken Sie hier, **um neue Einträge zu Ihrer Positiv-/Negativliste hinzuzufügen.**



Geben Sie in diesem Bildschirm die E-Mail-Adresse oder Domäne ein, die zur Positivliste hinzugefügt werden soll, und wählen Sie anschließend in der Drop-Down-Liste **Gewünschte Aktion** die Option **Zu Positivliste hinzufügen** aus.

Wenn die Nachricht, die blockiert wurde, nicht von einem Newsletter oder einer Massen-E-Mail stammt und Sie glauben, dass sie von TRITON AP-EMAIL falsch klassifiziert wurde, können Sie eine Kopie der Nachricht an spam@mailcontrol.com schicken. Das Spam-Rechercheteam bei Websense überprüft diese Nachrichten und aktualisiert den Erkennungsmechanismus gegebenenfalls entsprechend.

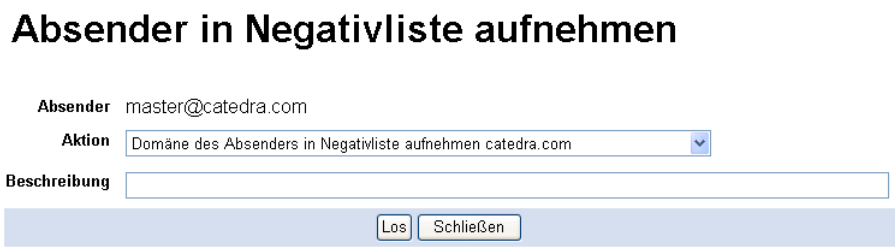
Warum hat TRITON AP-EMAIL die Spam-Nachrichten, die ich erhalten habe, nicht blockiert?

Websense aktualisiert ständig seinen Spam-Filtermechanismus, um neue Arten von Spam erkennen zu können. TRITON AP-EMAIL erkennt konsistent mehr als 99 Prozent aller Spam-E-Mails, die durch den Dienst geleitet werden. Spam ist jedoch subjektiv. Was für den einen Benutzer Spam ist, kann für den anderen eine legitime E-Mail sein.

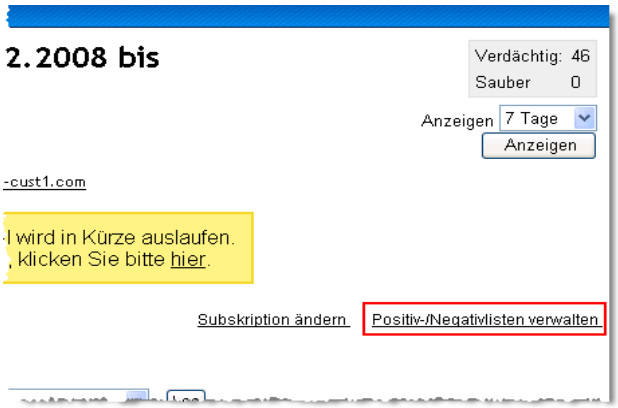
Um zu verhindern, dass TRITON AP-EMAIL Nachrichten eines bestimmten Absenders in der Zukunft weiterleitet, können Sie den Absender zu Ihrer Negativliste hinzufügen (sofern Ihnen Ihr Administrator hierzu die Berechtigung gegeben hat). E-Mails, die von Absendern in Ihrer Negativliste stammen, werden immer als Spam klassifiziert.

Sie können einen Absender zu Ihrer Negativliste hinzufügen, indem Sie die E-Mail im Nachrichtenbericht suchen, die Nachricht durch einen Klick in das Markierungsfeld auswählen und auf die Schaltfläche **In Negativliste aufnehmen** klicken.

Verwenden Sie im Bildschirm, der darauf angezeigt wird, die Drop-Down-Liste, um eine Aktion vorzunehmen: **E-Mail-Adresse des Absenders in Negativliste aufnehmen** oder **Domäne des Absenders in Negativliste aufnehmen**. Klicken Sie anschließend auf **Los**.

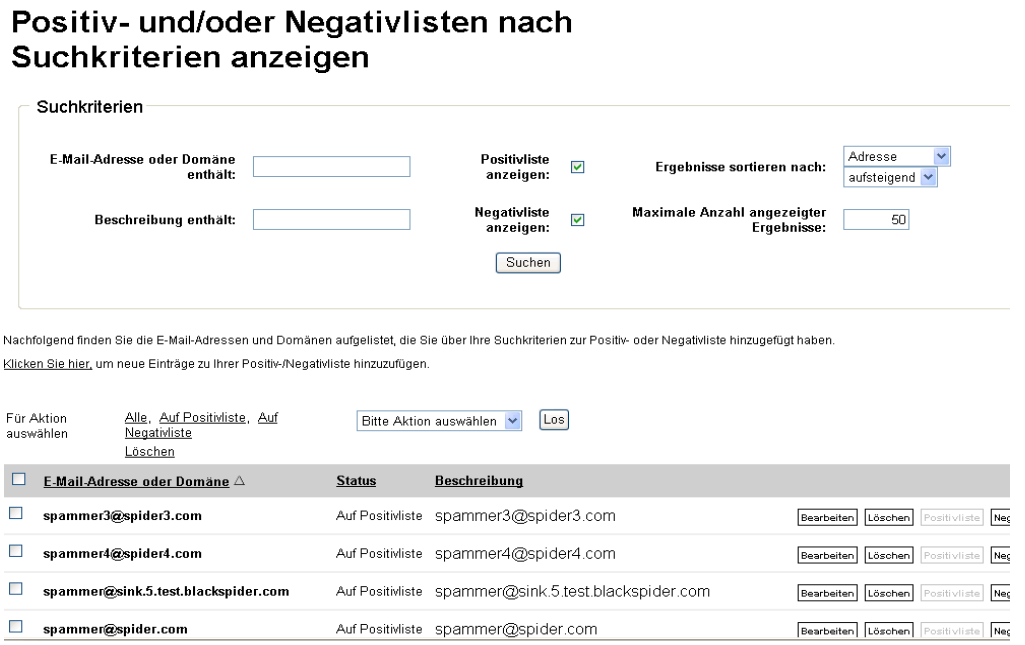


Sie können Ihre gesamte Negativliste anzeigen oder verwalten, indem Sie in Ihrem Nachrichtenbericht **Positiv-/Negativlisten verwalten** auswählen.

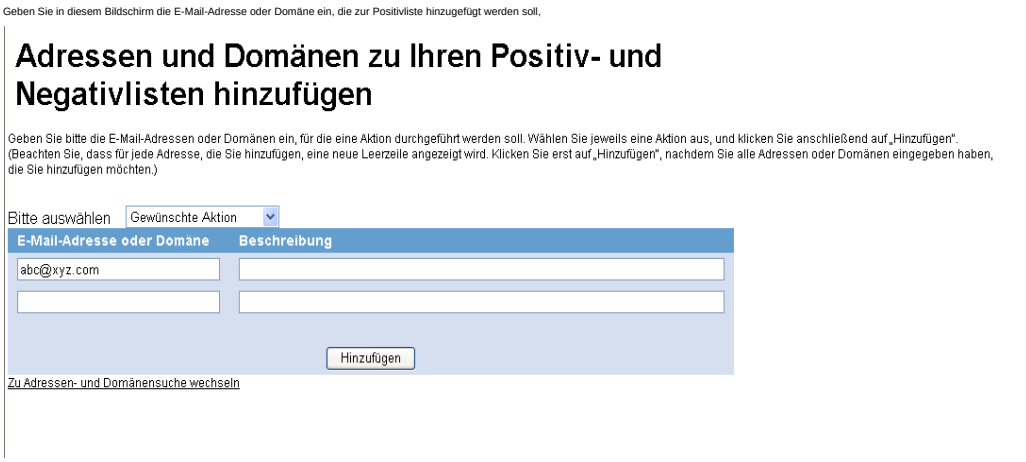


Im Bildschirm, der daraufhin angezeigt wird, können Sie Ihre Negativliste auf E-Mail-Adressen oder Domänen durchsuchen. Klicken Sie auf **Negativliste anzeigen,** geben Sie Suchkriterien ein, beispielsweise die Adresse, die Sie finden möchten, und

klicken Sie anschließend auf **Suchen**. Sie können angeben, wie die Ergebnisse sortiert werden sollen und wie viele Ergebnisse angezeigt werden sollen.



Wenn Sie eine Adresse zu Ihrer Negativliste hinzufügen möchten, die noch nicht darin vorhanden ist, klicken Sie auf den Link Klicken Sie hier, **um neue Einträge zu Ihrer Positiv-/Negativliste hinzuzufügen.**



Geben Sie in diesem Bildschirm die E-Mail-Adresse oder Domäne ein, die zur Negativliste hinzugefügt werden soll, und wählen Sie anschließend in der Drop-Down-Liste **Gewünschte Aktion** die Option **Zu Negativliste hinzufügen** aus.

Wenn Sie glauben, dass die Nachricht von TRITON AP-EMAIL falsch klassifiziert wurde, informieren Sie Websense bitte hierüber, wenn Sie die Option dazu erhalten. Dies hilft uns dabei, TRITON AP-EMAIL zu optimieren. Wenn Ihr Administrator diese Funktion zugelassen hat, finden Sie am Ende der Nachricht einen Link „Klicken

Sie hier, um diese Nachricht als Spam zu melden“. Wenn Sie auf den Link klicken, erhalten Sie eine Bestätigungsmeldung.

Da die Definition von Spam wie bereits erwähnt subjektiv ist, kann Websense nicht automatisch alle E-Mails, die dieser ähnlich sind, als Spam klassifizieren. Indem Sie die E-Mail an uns weiterleiten, helfen Sie uns, den Dienst zu optimieren. Letztendlich profitieren alle Kunden hiervon. Wenn Sie sicherstellen möchten, dass Sie keine weiteren E-Mails von der entsprechenden Absenderadresse erhalten möchten, fügen Sie diese bitte zu Ihrer Negativliste hinzu.

Empfehlungen für den Umgang mit Spam

Situation	Empfohlene Aktion
Sie erhalten E-Mails von einer einzelnen Person, von der Sie keine weiteren E-Mail erhalten möchten.	Fügen Sie den Absender zu Ihrer persönlichen Negativliste hinzu**.** (Diese Funktion muss von Ihrem Administrator aktiviert werden.)
Sie erhalten eine E-Mail-Nachricht, die Sie nicht als Spam betrachten.	Fügen Sie den Absender zu Ihrer persönlichen Positivliste hinzu**.** (Diese Funktion muss von Ihrem Administrator aktiviert werden.)
Sie erhalten unangeforderte Werbe-E-Mails.	Klicken Sie auf den Link „Diese E-Mail als Spam melden“ am Ende der E-Mail-Nachricht. Die Verwendung dieses Dienstes hilft uns dabei, Spam in Zukunft noch besser zu erkennen. Bei reinen Text-E-Mails, in denen dieser Link nicht angezeigt wird, können Sie die Nachricht an spam@mailcontrol.com weiterleiten.
Sie möchten elektronische Newsletter oder Marketing-Literatur, die Sie zuvor erhalten haben, nicht mehr erhalten.	Kündigen Sie Ihr Abonnement des Mailing-Dienstes, oder fügen Sie den Absender zu Ihrer Negativliste hinzu. Klicken Sie nicht auf den Link „Diese E-Mail als Spam melden“, da andere Empfänger derartige E-Mails nicht als Spam betrachten werden.
Sie erhalten elektronische Newsletter oder Angebote eines Unternehmens, mit dem Sie zwar Kontakt hatten, von dem Sie allerdings keine entsprechende Kommunikation erwarten. (Möglicherweise haben Sie versehentlich zugestimmt, in deren Mailing-Liste aufgenommen zu werden.)	