

ESA - Zusätzliche E-Mail-Header für Verschlüsselung

Inhalt

[Einführung](#)

[Umschlagschlüssel-Caching für Offline-Öffnen aktivieren](#)

[JavaScript-freie Umschläge aktivieren](#)

[Nachrichtenablauf aktivieren](#)

[Entschlüsselungs-Applet deaktivieren](#)

[Zusätzliche Informationen](#)

Einführung

Dieses Dokument beschreibt zusätzliche E-Mail-Header, die über Content- oder Nachrichtenfilter der Cisco E-Mail Security Appliance (ESA) implementiert werden können.

Umschlagschlüssel-Caching für Offline-Öffnen aktivieren

Um einen registrierten Umschlag mit aktivierter Envelope Key-Caching zu senden, fügen Sie diesen Header in die Nachricht ein:

```
X-PostX-Remember-Envelope-Key-Checkbox: true
```

Das Kontrollkästchen "Kennwort für diesen Umschlag speichern" wird auf dem registrierten Umschlag angezeigt.

JavaScript-freie Umschläge aktivieren

Um einen registrierten Umschlag ohne JavaScript zu senden, fügen Sie diesen Header in die Nachricht ein:

```
X-PostX-Use-Script: false
```

Wenn der Empfänger die Anlage **securedoc.html** öffnet, wird der registrierte Umschlag mit dem Link "Online öffnen" angezeigt, und die Schaltfläche "Öffnen" ist deaktiviert.

Nachrichtenablauf aktivieren

Um eine Nachricht so zu konfigurieren, dass sie 24 Stunden nach dem Senden abläuft, fügen Sie

diesen Header in die Nachricht ein:

```
X-PostX-ExpirationDate: +24:00:00
```

Der Empfänger kann den Inhalt der verschlüsselten Nachricht während des 24-Stunden-Zeitraums nach dem Senden öffnen und anzeigen. Danach zeigt der registrierte Umschlag eine Meldung an, dass der Umschlag abgelaufen ist.

Entschlüsselungs-Applet deaktivieren

Um das Entschlüsselungs-Applet zu deaktivieren und den Nachrichtenanhang auf dem Schlüsselservers entschlüsseln zu lassen, fügen Sie diesen Header in die Nachricht ein:

```
X-PostX-Suppress-Applet-For-Open: true
```

Hinweis: Wenn Sie das Entschlüsselungs-Applet deaktivieren, dauert das Öffnen der Nachricht möglicherweise länger, aber sie ist nicht von der Browserumgebung abhängig.

Zusätzliche Informationen

MIME-Header (Multipurpose Internet Mail Extensions)

	Beschreibung	Wert
X-PostX-Reply-fähig	Gibt an, ob eine sichere Antwort für die Nachricht aktiviert werden soll, und zeigt die Schaltfläche Antworten in der Nachrichtenleiste an. Dieser Header fügt der Nachricht eine Verschlüsselungseinstellung hinzu.	Ein boolescher Wert für Anzeige der Schaltfläche Antworten. Legen Sie true fest, um die Schaltfläche anzuzeigen. Der Standardwert ist false.
X-PostX-Reply-All-Enabled	Gibt an, ob eine sichere "Antwort an alle" für die Nachricht aktiviert werden soll, und zeigt die Schaltfläche Alle antworten in der Nachrichtenleiste an. Dieser Header überschreibt die Standardprofileinstellung.	Ein boolescher Wert für Anzeige der Schaltfläche Alle antworten. Legen Sie true fest, um die Schaltfläche anzuzeigen. Der Standardwert ist false.
X-PostX-Forward-fähig	Gibt an, ob die sichere Nachrichtenweiterleitung aktiviert werden soll, und zeigt die Weiterleitungstaste in der Nachrichtenleiste an. Dieser Header überschreibt die Standardprofileinstellung.	Ein boolescher Wert für Anzeige der Schaltfläche Weiterleiten. Legen Sie true fest, um die Schaltfläche anzuzeigen. Der Standardwert ist false.
X-PostX-Send-Return-Receipt	Gibt an, ob Lesebestätigungen aktiviert werden sollen. Der Absender erhält eine Quittung, wenn Empfänger den sicheren Umschlag öffnen. Dieser Header überschreibt die Standardprofileinstellung.	Ein boolescher Wert für Senden einer Lesebestätigung. Legen Sie true fest, um die Schaltfläche anzuzeigen. Der Standardwert ist false.
X-PostX-Ablaufdatum	Definiert das Ablaufdatum eines registrierten Umschlags, bevor dieser gesendet wird. Der Schlüsselservers	Ein Zeichenfolgenwert, das relative Datum oder relative Uhrzeit enthält.

beschränkt den Zugriff auf den registrierten Umschlag nach dem Ablaufdatum. Der registrierte Umschlag zeigt eine Meldung an, die angibt, dass die Nachricht abgelaufen ist. Dieser Header fügt der Nachricht eine Verschlüsselungseinstellung hinzu. Wenn Sie den Cisco Registered Envelope Service verwenden, können Sie sich bei der Website unter <http://res.cisco.com> anmelden und die Nachrichtenverwaltungsfunktionen verwenden, um das Ablaufdatum von Nachrichten nach dem Senden festzulegen, anzupassen oder zu löschen.

Verwenden Sie das Format +HH:MM:SS für relative Stunden, Minuten und Sekunden und das Format +D für relative Tage. Standardmäßig gibt es kein Ablaufdatum.

X-PostX-ReadNotificationDate

Definiert das Datum für registrierte Umschläge, die vor dem Senden gelesen werden. Der lokale Schlüsselservers generiert eine Benachrichtigung, wenn der registrierte Umschlag bis zu diesem Datum nicht gelesen wurde. Registrierte Umschläge mit diesem Header funktionieren nicht mit dem Cisco Registered Envelope Service, sondern nur mit einem lokalen Schlüsselservers. Dieser Header fügt der Nachricht eine Verschlüsselungseinstellung hinzu.

Ein Zeichenfolgenwert, das das relative Datum oder die relative Uhrzeit enthält. Verwenden Sie das Format +HH:MM:SS für relative Stunden, Minuten und Sekunden und das Format +D für relative Tage. Standardmäßig gibt es kein Ablaufdatum.

X-PostX-Suppress-Applet-zum-Öffnen

Gibt an, ob das Entschlüsselungs-Applet deaktiviert werden soll. Das Entschlüsselungs-Applet bewirkt, dass Nachrichtenanhänge in der Browserumgebung geöffnet werden. Wenn Sie das Applet deaktivieren, wird der Nachrichtenanhang auf dem Schlüsselservers entschlüsselt. Wenn Sie diese Option deaktivieren, dauert das Öffnen von Nachrichten möglicherweise länger, jedoch nicht abhängig von der Browserumgebung. Dieser Header überschreibt die Standardprofileinstellung.

Ein boolescher Wert, der angibt, ob das Entschlüsselungs-Applet deaktiviert werden soll. Legen Sie true fest, um das Applet zu deaktivieren. Der Standardwert ist false.

X-PostX-Use-Script

Gibt an, ob JavaScript-freie Umschläge gesendet werden sollen. Ein JavaScript-freier Umschlag ist ein registrierter Umschlag, der das JavaScript nicht enthält, mit dem Umschläge lokal auf dem Computer des Empfängers geöffnet werden. Der Empfänger muss entweder die Open Online-Methode oder die Open by Forwarding-Methode verwenden, um die Nachricht anzuzeigen. Verwenden Sie diesen Header, wenn das Gateway

Ein boolescher Wert für die Angabe, ob das JavaScript-Applet enthalten sein soll oder nicht. Legen Sie false fest, um einen JavaScript-freien Umschlag zu senden. Der Standardwert ist true.

X-PostX-Remember-Envelope-Key-
Kontrollkästchen

einer Empfängerdomäne JavaScript entfernt und die verschlüsselte Nachricht unopbar macht. Dieser Header fügt der Nachricht eine Verschlüsselungseinstellung hinzu. Gibt an, ob das Offline-Öffnen von Umschlägen durch Envelope-spezifisches Schlüssel-Caching ermöglicht werden soll. Bei der Zwischenspeicherung von Umschlagschlüsseln wird der Entschlüsselungsschlüssel für einen bestimmten Umschlag auf dem Computer des Empfängers zwischengespeichert, wenn der Empfänger das richtige Kennwort eingibt und das Kontrollkästchen "Kennwort für diesen Umschlag speichern" aktiviert. Danach muss der Empfänger kein Kennwort mehr eingeben, um den Umschlag auf dem Computer erneut zu öffnen. Dieser Header fügt der Nachricht eine Verschlüsselungseinstellung hinzu.

Ein boolescher Wert, der angibt, ob die Zwischenspeicherung von Umschlagschlüsseln aktiviert und das Kontrollkästchen "Kennwort für diesen Umschlag speichern" aktiviert werden soll. Der Standardwert ist false.