

암호화를 위한 ESA 추가 이메일 헤더

목차

[소개](#)

[오프라인 열기에 봉투 키 캐싱 사용](#)

[JavaScript-Free 봉투 사용](#)

[메시지 만료 사용](#)

[암호 해독 애플릿 비활성화](#)

[추가 정보](#)

소개

이 문서에서는 Cisco ESA(Email Security Appliance)의 콘텐츠 또는 메시지 필터를 통해 구현할 수 있는 추가 이메일 헤더에 대해 설명합니다.

오프라인 열기에 봉투 키 캐싱 사용

봉투 키 캐싱이 활성화된 등록된 봉투를 보내려면 다음 헤더를 메시지에 삽입합니다.

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

"Remember the password for this envelope" 확인란이 Registered Envelope에 표시됩니다.

JavaScript-Free 봉투 사용

JavaScript가 없는 등록된 봉투를 보내려면 다음 헤더를 메시지에 삽입합니다.

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

수신자가 `securedoc.html` 첨부 파일을 열면 등록된 봉투가 온라인 열기 링크와 함께 표시되고 열기 버튼이 비활성화됩니다.

메시지 만료 사용

메시지를 보낸 후 24시간 후에 만료되도록 메시지를 구성하려면 다음 헤더를 메시지에 삽입합니다.

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

수신자는 사용자가 메시지를 보낸 후 24시간 동안 암호화된 메시지의 내용을 열고 볼 수 있습니다. 그런 다음 Registered Envelope에 봉투가 만료되었음을 나타내는 메시지가 표시됩니다.

암호 해독 애플릿 비활성화

암호 해독 애플릿을 비활성화하고 키 서버에서 메시지 첨부 파일을 해독하려면 다음 헤더를 메시지에 삽입합니다.

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

참고: 암호 해독 애플릿을 비활성화하면 메시지를 여는 데 시간이 더 걸릴 수 있지만 브라우저 환경에 종속되지 않습니다.

추가 정보

MIME(Multipurpose Internet Mail Extensions) 헤더

	설명	가치
X-PostX-Reply-Enabled	메시지에 대해 안전한 회신을 활성화할지 여부를 나타내며 메시지 표시줄에 회신 단추를 표시합니다. 이 헤더는 메시지에 암호화 설정을 추가합니다.	회신 단추를 표시할지 여부를 나타내는 부울 값입니다. 단추를 표시하려면 true로 설정합니다. 기본값은 false입니다.
X-PostX-Reply-All-Enabled	메시지에 대해 안전한 "전체 회신" 활성화 여부를 나타내며 메시지 표시줄에 모두 회신 단추를 표시합니다. 이 헤더는 기본 프로파일 설정을 재정의합니다.	[모두 회신] 단추를 표시할지 여부를 나타내는 부울 값입니다. 단추를 표시하려면 true로 설정합니다. 기본값은 false입니다.
X-PostX-전달 사용	보안 메시지 전달을 활성화할지 여부를 나타내며 메시지 표시줄에 전달 단추를 표시합니다. 이 헤더는 기본 프로파일 설정을 재정의합니다.	앞으로 단추를 표시할지 여부를 나타내는 부울 값입니다. 단추를 표시하려면 true로 설정합니다. 기본값은 false입니다.
X-PostX-Send-Return-Receipt	읽음 확인 기능을 사용할지 여부를 나타냅니다. 수신자가 Secure Envelope(보안 봉투)를 열면 발신자가 영수증을 받습니다. 이 헤더는 기본 프로파일 설정을 재정의합니다.	읽음 확인 메일을 보낼지 여부를 나타내는 부울 값입니다. 단추를 표시하려면 true로 설정합니다. 기본값은 false입니다.
X-PostX-만료일	등록된 봉투의 만료 날짜를 전송하기 전에 정의합니다. 키 서버는 만료 날짜 이후에 등록된 봉투에 대한 액세스를 제한합니다. 등록된 봉투에 메시지가 만료되었음을 나타내는 메시지가 표시됩니다. 이 헤더는 메시지에 암호화 설정을 추가합니다. Cisco Registered Envelope Service를 사용하는 경우 http://res.cisco.com 의 웹 사이트로 그인하여 메시지 관리 기능을 사용하여 메시지를 보낸 후 메시지의 만료일을 설정, 조정 또는 제거할 수 있습니다.	상대 날짜 또는 시간을 포함하는 문자열 값입니다. 상적인 시간, 분, 초의 경우 +HH:MM:SS 형식, 상대적 일의 경우 +D 형식을 사용합니다. 기본적으로 만료 날짜는 없습니다.
X-PostX-ReadNotificationDate	등록된 봉투가 전송되기 전의 "읽기 기준" 날짜를 정의합니다. 로컬 키 서버는 등록된 봉투를 이 날짜까지 읽지 않은 경우 알림을 생성합니다. 이 헤더의 등록된 봉투는	상대 날짜 또는 시간을 포함하는 문자열 값입니다. 상적인 시간, 분, 초의 경우 +HH:MM:SS 형식, 상대적

Cisco Registered Envelope Service에서 작동하지 않으며 로컬 키 서버만 사용할 수 있습니다. 이 헤더는 메시지에 암호화 설정을 추가합니다.

암호 해독 애플릿을 비활성화할지 여부를 나타냅니다. 암호 해독 애플릿을 사용하면 브라우저 환경에서 메시지 첨부 파일을 열 수 있습니다. 애플릿을 비활성화하면 메시지 첨부 파일이 키 서버에서 해독됩니다. 이 옵션을 비활성화하면 메시지를 여는 데 시간이 오래 걸릴 수 있지만 브라우저 환경에 종속되지 않습니다. 이 헤더는 기본 프로파일 설정을 재정의합니다.

JavaScript 제외 봉투를 보낼지 여부를 나타냅니다. JavaScript가 없는 봉투는 수신자의 컴퓨터에서 로컬로 봉투를 여는 데 사용되는 JavaScript가 포함되지 않은 등록된 봉투입니다. 수신자는 메시지를 보려면 Open Online 메서드 또는 Open by Forwarding 메서드를 사용해야 합니다. 수신인 도메인의 게이트웨이가 JavaScript를 제거하고 암호화된 메시지를 비활성화하는 경우 이 헤더를 사용합니다. 이 헤더는 메시지에 암호화 설정을 추가합니다.

봉투의 오프라인 오프닝을 위해 봉투 특정 키 캐싱을 허용할지 여부를 나타냅니다. 봉투 키 캐싱을 사용하면 수신자가 올바른 비밀번호를 입력하고 "Remember the password for this envelope" 확인란을 선택하면 특정 봉투에 대한 암호 해독 키가 수신자의 컴퓨터에 캐시됩니다. 그런 다음 수신자는 컴퓨터에서 봉투를 다시 열기 위해 비밀번호를 다시 입력할 필요가 없습니다. 이 헤더는 메시지에 암호화 설정을 추가합니다.

일의 경우 +D 형식을 사용합니다. 기본적으로 만료 날짜는 없습니다.

해독 애플릿을 사용하지 않도록 설정할지 여부를 나타내는 부울 값입니다. 애플릿을 사용하지 않도록 설정하려면 true로 설정합니다. 기본값은 false입니다.

JavaScript 애플릿을 포함해야 하는지 여부에 대한 부울 값입니다. JavaScript 없는 봉투를 전송하려면 false로 설정합니다. 기본값은 true입니다.

봉투 키 캐싱을 활성화하 "Remember the password for this envelope" 확인란 표시할지 여부를 나타내는 부울 값입니다. 기본값은 false입니다.

X-PostX-Suppress-Applet-For-Open

X-PostX-사용 스크립트

X-PostX-Remember-Envelope-Key-확인란