ESA CRES 암호화 프로파일에서 보안 레벨 구성

목차

소개

이 문서에서는 ESA(Email Security Appliance) 내의 Cisco CRES(Registered Envelope Service Encryption) 프로파일 컨피그레이션에 대해 설명하며, 허용되는 다양한 보안 레벨에 중점을 둡니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- ESA 기본 컨피그레이션
- 콘텐츠 필터 컨피그레이션 기반 암호화
- Cisco 등록 봉투 서비스

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

CRES 프로파일 생성은 ESA를 통한 암호화 서비스 활성화 및 사용을 위한 핵심 작업이다. 여러 프로파일을 생성하기 전에 CRES 어카운트 생성과 함께 ESA에 대해 프로비저닝된 전체 어카운트가 있는지 확인합니다.

둘 이상의 프로필이 있을 수 있으며 각 프로필은 다른 보안 수준으로 구성할 수 있습니다. 이를 통해 네트워크는 도메인, 사용자 또는 그룹별로 각기 다른 보안 수준을 유지할 수 있습니다.

구성

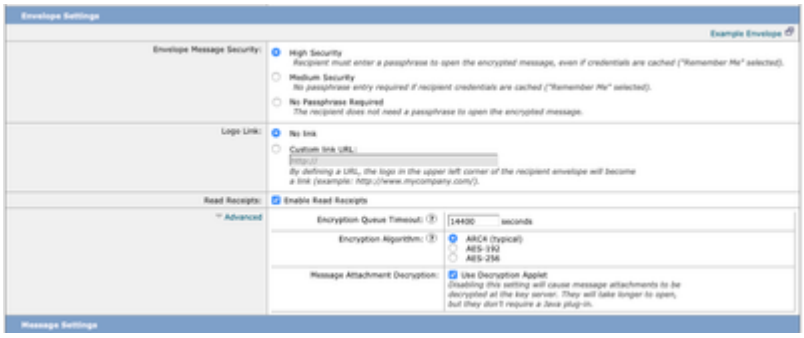
encryptionconfig CLI 명령을 사용하거나 GUI에서 Security Services(보안 서비스) > Cisco IronPort Email Encryption(Cisco IronPort 이메일 암호화)을 통해 암호화 프로파일을 활성화하고 구성할 수 있습니다.

GUI에서 구성

ESA에서 Security Services(보안 서비스) > Cisco IronPort Email Encryption(Cisco IronPort 이메일 암호화) > Add Encryption Profile(암호화 프로파일 추가)로 이동합니다.

Encryption Profile Settings(암호화 프로파일 설정) 화면이 표시됩니다. 프로필 이름 및 나머지 컨피그레이션은 사용자 지정할 수 있으며 조직의 식별 태그 또는 방법에 따라 달라집니다.

이미지에 표시된 대로 프로파일당 보안 수준을 정의하는 컨피그레이션은 Envelope Settings(봉투 설정)입니다.



참고: 프로필 이름에는 다음이 포함되는 것이 좋습니다. 콘텐츠 필터 생성 및 확인에서 빠른 식별을 위해 구성된 보안 수준 또는 프로필이 연결된 그룹의 이름과 일치시키기 위해 "높음", "낮음" 등의 작업을 수행합니다.

ESA에서 허용하는 세 가지 보안 수준은 다음과 같습니다.

- 높은 보안 수준: 수신자가 암호화된 메시지를 열려면 항상 암호를 입력해야 합니다.
- 중간 보안: 수신인 자격 증명이 캐시된 경우 수신인은 암호화된 메시지를 열기 위해 자격 증명을 입력할 필요가 없습니다.
- 암호 사용 안 함: 이는 암호화된 메시지 보안의 최하위 레벨입니다. 수신자는 암호화된 메시지를 열기 위해 암호를 입력할 필요가 없습니다. 암호로 보호되지 않은 봉투에 대해서는 여전히 읽기 확인, 전체 회신 보안 및 메시지 전달 보안 기능을 활성화할 수 있습니다.

다음 객체에 대해 서로 다른 보안 레벨을 구성할 수 있습니다.

봉투 메시지 보안:

- · 높은 보안
- 중간 보안
- 패스프레이즈 불필요

로고 링크: 사용자가 조직의 URL을 열고 해당 로고를 클릭할 수 있도록, 로고에 대한 링크를 추가할 수 있습니다. 다음 옵션 중에서 선택합니다.

- 링크가 없습니다. 라이브 링크는 메시지 봉투에 추가되지 않습니다.
- 사용자 지정 링크 URL. 메시지 봉투에 라이브 링크를 추가하려면 URL을 입력합니다.

읽음 확인: 이 옵션을 활성화하면 수신자가 보안 봉투를 열 때 발신자가 수신 메시지를 수신합니다. 선택 사항입니다.

고급:

암호화 대기열 시간 초과: 메시지가 시간 초과되기 전에 암호화 대기열에 있을 수 있는 시간(초)을 입력합니다. 메시지가 시간 초과되면 어플라이언스는 메시지를 반송하고 발신자에게 알림을 전송합니다.

암호화 알고리즘:

- ARC4. ARC4는 가장 일반적인 선택이며, 메시지 수신자에 대한 암호 해독 지연을 최소화하면서 강력한 암호화를 제공합니다.
- AES. AES는 더 강력한 암호화를 제공하지만 해독에 더 오래 걸리므로 수신자에게 지연이 발생합니다. AES는 일반적으로 정부 및 은행 애플리케이션에서 사용됩니다.

메시지 첨부 파일 암호 해독: 해독 애플릿을 활성화 또는 비활성화합니다. 이 옵션을 활성화하면 브라우저 환경에서 메시지 첨부 파일이 열립니다. 이 옵션을 비활성화하면 메시지 첨부 파일이 키 서버에서 해독됩니다. 기본적으로 Java 애플릿은 봉투에서 비활성화됩니다.

참고: 가장 많이 사용되는 브라우저는 보안상의 이유로 Java Applet을 비활성화했습니다.

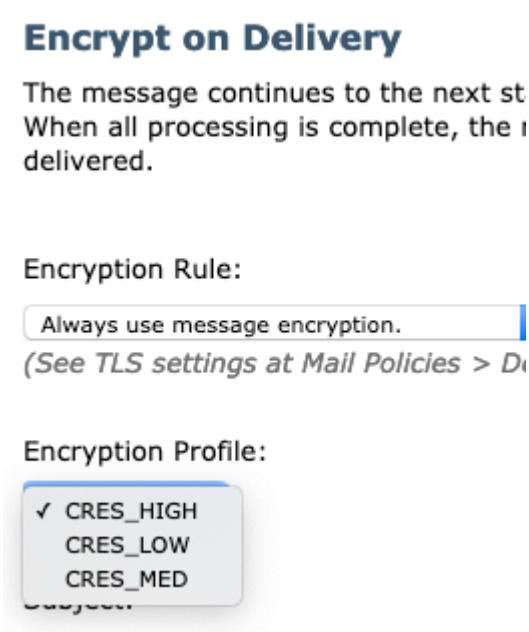
암호화 프로파일이 생성되면 이미지에 표시된 대로 프로비저닝되었는지 확인합니다.

이러한 각 프로필을 적용하려면 콘텐츠 필터를 통해 연결해야 합니다.

주의: 콘텐츠 필터에서 프로필을 호출하지 않으면 암호화 설정을 적용할 수 없습니다.

ESA에서 Mail Policies(메일 정책) > Outgoing Content Filters(발신 콘텐츠 필터) > Add a filter(필터 추가)로 이동합니다

사용자, 주체, 그룹, 발신자 등의 상태가 필터 내에 구성되었으면 이미지에 표시된 대로 발신 필터의 암호화 수준을 정의합니다.



⚠ 주의: 제대로 작동하려면 모든 콘텐츠 필터를 발신 메일 정책과 연결해야 합니다.

✎ 참고: 호스팅된 키 서비스에 대해 여러 암호화 프로필을 구성할 수 있습니다. 조직에 여러 브랜드가 있는 경우 이를 통해 PXE 엔벨로프에 대한 키 서버에 저장된 서로 다른 로고를 참조할 수 있습니다.

CLI에서 컨피그레이션

ESA CLI에서 encryptionconfig 명령을 입력합니다.

```
ESA.com> encryptionconfig

IronPort Email Encryption: Enabled

Choose the operation you want to perform:
- SETUP - Enable/Disable IronPort Email Encryption
- PROFILES - Configure email encryption profiles
- PROVISION - Provision with the Cisco Registered Envelope Service

[]> profiles

Proxy: Not Configured

Profile Name         Key Service            Proxied     Provision Status
------------         -----------            -------     ----------------
HIGH-CRES              Hosted Service         No          Not Provisioned
Choose the operation you want to perform:
- NEW - Create a new encryption profile
- EDIT - Edit an existing encryption profile
- DELETE - Delete an encryption profile
- PRINT - Print all configuration profiles
- CLEAR - Clear all configuration profiles
- PROXY - Configure a key server proxy
[]> new
```

```
1. Cisco Registered Envelope Service
2. IronPort Encryption Appliance (in network)
Choose a key service:
[1]>

Enter a name for this encryption profile:
[]> HIGH

Current Cisco Registered Key Service URL: https://res.cisco.com
Do you wish to alter the Cisco Registered Envelope Service URL? [N]> N

1. ARC4
2. AES-192
3. AES-256
Please enter the encryption algorithm to use when encrypting envelopes:
[1]>

1. Use envelope service URL with HTTP (Recommended). Improves performance for opening envelopes.
2. Use the envelope service URL with HTTPS.
3. Specify a separate URL for payload transport.
Configure the Payload Transport URL
[1]>

1. High Security (Recipient must enter a passphrase to open the encrypted message, even if credentials
2. Medium Security (No passphrase entry required if recipient credentials are cached ("Remember Me" sel
3. No Passphrase Required (The recipient does not need a passphrase to open the encrypted message.)
Please enter the envelope security level:
[1]>

Would you like to enable read receipts? [Y]>

Would you like to enable "Secure Reply All"? [N]> y

Would you like to enable "Secure Forward"? [N]> y

Enter a URL to serve as a link for the envelope logo image (may be blank):
[]>

Would you like envelopes to be displayed in a language other than English ? [N]>

Enter the maximum number of seconds for which a message could remain queued waiting to be encrypted. De
[14400]>

Enter the subject to use for failure notifications:
[[ENCRYPTION FAILURE]]>

Please enter file name of the envelope attached to the encryption notification:
[securedoc_${date}T${time}.html]>


A Cisco Registered Envelope Service profile "HIGH" was added.

   1. Commit this configuration change before continuing.
   2. Return to the encryptionconfig menu and select PROVISION to complete
the configuration.

Proxy: Not Configured

Profile Name         Key Service            Proxied     Provision Status
------------         -----------            -------     ----------------
HIGH-CRES            Hosted Service         No          Not Provisioned
```

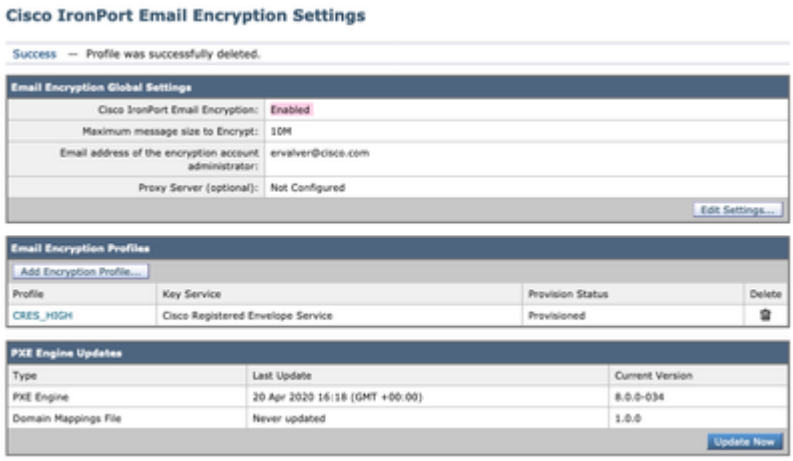
```
LOW-CRES              Hosted Service         No          Not Provisioned

Choose the operation you want to perform:
- SETUP - Enable/Disable IronPort Email Encryption
- PROFILES - Configure email encryption profiles
- PROVISION - Provision with the Cisco Registered Envelope Service

[]> provision
```

다음을 확인합니다.

설정이 올바르게 작동하는지 확인하려면 이 섹션을 활용하십시오.

GUI에서 확인

그림과 같이 ESA에서 Security Services(보안 서비스) > Cisco IronPort Email Encryption(Cisco IronPort 이메일 암호화)으로 이동합니다.



참고: 암호화가 활성화되고 구성된 프로파일이 프로비저닝되었는지 확인합니다. 그림과 같이.

CLI에서 확인

CLI에서 encryptconfig 및 type profiles 명령을 입력합니다.

```
ESA.com> encryptionconfig

IronPort Email Encryption: Enabled

Choose the operation you want to perform:
- SETUP - Enable/Disable IronPort Email Encryption
- PROFILES - Configure email encryption profiles
- PROVISION - Provision with the Cisco Registered Envelope Service
[]> profiles

Proxy: Not Configured
```

```
Profile Name         Key Service           Proxied     Provision Status
------------         -----------           -------     ----------------
CRES_HIGH             Hosted Service        No          Provisioned
```

참고: 암호화가 활성화되고 구성된 프로파일이 프로비저닝되었는지 확인합니다. 그림과 같이.

문제 해결

이 섹션에서는 설정 문제 해결을 위해 사용할 수 있는 정보를 제공합니다.

ESA에서 System Administration(시스템 관리) > feature keys(기능 키)로 이동합니다

기능 키가 적용되어 활성 상태인지 확인합니다. 주요 내용: IronPort 이메일 암호화가 활성화되어 있어야 합니다.

ESA에서 Security Services(보안 서비스) > Cisco IronPort Email Encryption(Cisco IronPort 이메일 암호화)으로 이동합니다.

암호화 서비스가 제대로 활성화되었는지 확인합니다.

이미지에 표시된 대로 암호화 프로파일이 Not Provisioned(프로비저닝되지 않음) 상태가 아닌지 확인합니다.

Profile	Key Service	Provision Status
HIGH	Cisco Registered Envelope Service	Not Provisioned
LOW	Cisco Registered Envelope Service	Not Provisioned
MEDIUM	Cisco Registered Envelope Service	Not Provisioned

이미지에 표시된 대로 엔진 마지막 업데이트를 확인합니다.

PXE Engine Updates		
Type	Last Update	Current Version
PXE Engine	21 Jan 2020 16:01 (GMT +00:00)	7.2.1-015

Message Tracking(메시지 추적) 세부사항에서 오류가 표시되는지 확인합니다.

가장 일반적인 오류:

```
5.x.3 - Temporary PXE Encryption failure
```

해결책: 현재 서비스를 사용할 수 없거나 서비스에 연결할 수 없습니다. 연결 및 네트워크 문제를 확인합니다.

```
5.x.3 - PXE Encryption failure. (Message could not be encrypted due to a system configuration issue. Pl
```

해결책: 이 오류는 다음과 관련이 있습니다.

- 라이센스 문제. 기능 키를 확인하십시오.
- 사용된 프로필이 프로비저닝되지 않았습니다. 콘텐츠 필터 및 프로비저닝에 구성된 프로필을 추적하는 메시지에서 식별
- 콘텐츠 필터와 연결된 프로필이 없습니다. 암호화 프로파일이 삭제되거나 다른 이름으로 수정되는 경우도 있습니다. 구성된 콘텐츠 필터가 연결된 프로필을 찾을 수 없습니다.

```
5.x.3 - PXE Encryption failure. (Error 30 - The message has an invalid "From" address.)
```

```
5.x.3 - PXE Encryption failure. (Error 102 - The message has an invalid "To" address.)
```

해결책: 정기적으로 이 문제는 내부 보낸 사람의 전자 메일 클라이언트(예: Outlook)가 잘못된 "보낸 사람"/"받는 사람" 주소가 포함된 받는 사람의 전자 메일 주소를 자동 채우므로 발생합니다.

일반적으로 이는 이메일 주소 주위의 따옴표나 이메일 주소의 다른 잘못된 문자로 인해 발생합니다
.

관련 정보

- 최종 사용자 설명서
- 기술 지원 및 문서 – Cisco Systems

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.