# 라우터에서 사전 공유 키 암호화 구성

## 목차



## 소개

이 문서에서는 라우터에서 현재 및 새 사전 공유 키의 암호화를 설정하는 방법에 대해 설명합니다.

## 사전 요구 사항

### 요구 사항

이 문서에 대한 특정 요건이 없습니다.

### 사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 버전을 기반으로 합니다.

- Cisco IOS XE® 소프트웨어 릴리스 16.9

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.

### 표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참조하십시오.

## 배경 정보

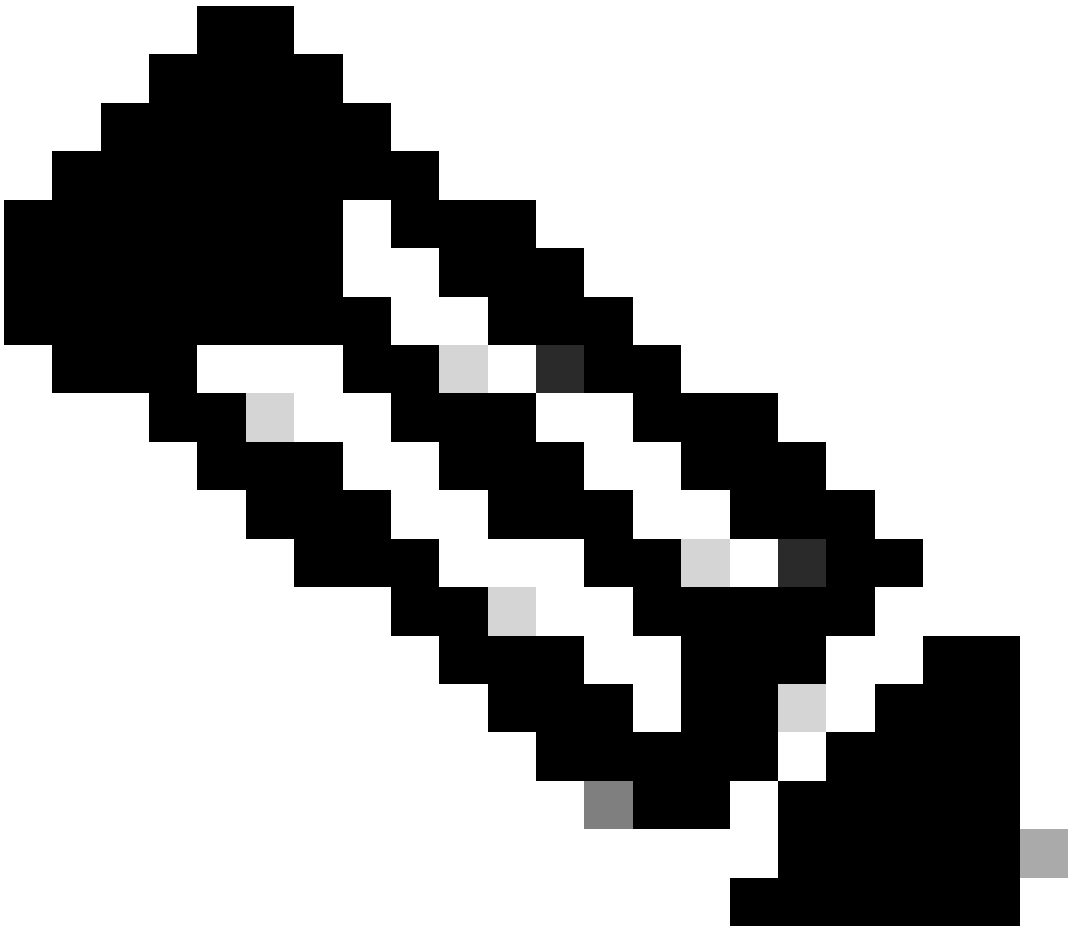
Cisco IOS Software Release 12.3(2)T 코드에는 라우터가 ISAKMP(Internet Security Association

and Key Management Protocol) 사전 공유 키를 비휘발성 RAM, NVRAM(Non-Volatile RAM)의 보안 유형 6 형식으로 암호화하는 기능이 도입되었습니다. 암호화할 사전 공유 키는 표준, ISAKMP 키링에서, 어그레시브 모드에서 또는 EzVPN(Easy VPN) 서버 또는 클라이언트 설정에서 그룹 암호로 구성할 수 있습니다.

## 구성

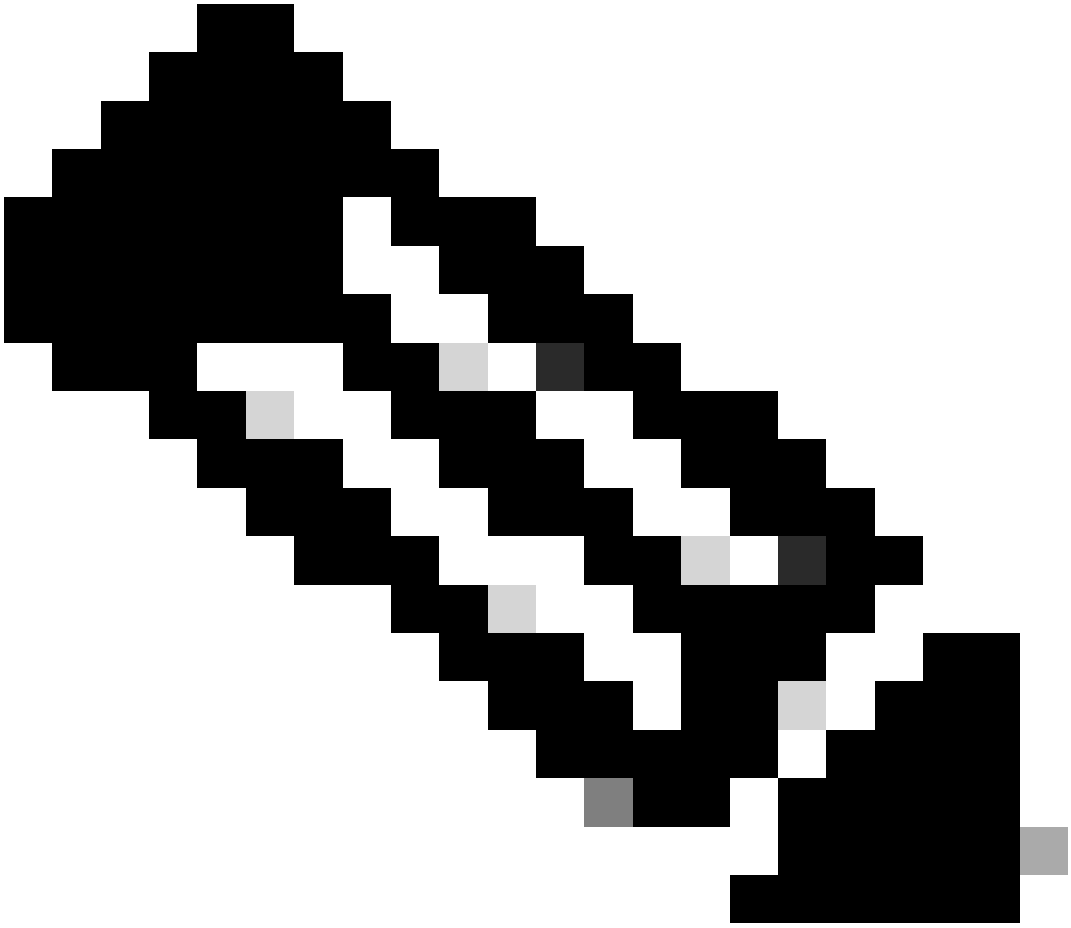
이 섹션에서는 이 문서에서 설명하는 기능을 구성하는 데 사용할 수 있는 정보를 제공합니다.

---



참고: 이 섹션에서 사용되는 명령에 대한 자세한 내용을 보려면 명령 조회 도구를 사용하십시오.

---



참고: 등록된 Cisco 사용자만 내부 Cisco 툴 및 정보에 액세스할 수 있습니다.

---

사전 공유 키 암호화를 활성화하기 위해 다음 두 명령을 도입했습니다.

- key config-key password-encryption [기본 키]
- 비밀번호 암호화 aes

[기본 키]는 AES(Advance Encryption Standard) 대칭 암호를 사용하여 라우터 컨피그레이션의 다른 모든 키를 암호화하는 데 사용되는 암호/키입니다. 기본 키는 라우터 컨피그레이션에 저장되지 않으며 라우터에 연결되어 있는 동안에는 어떠한 방식으로도 보거나 가져올 수 없습니다.

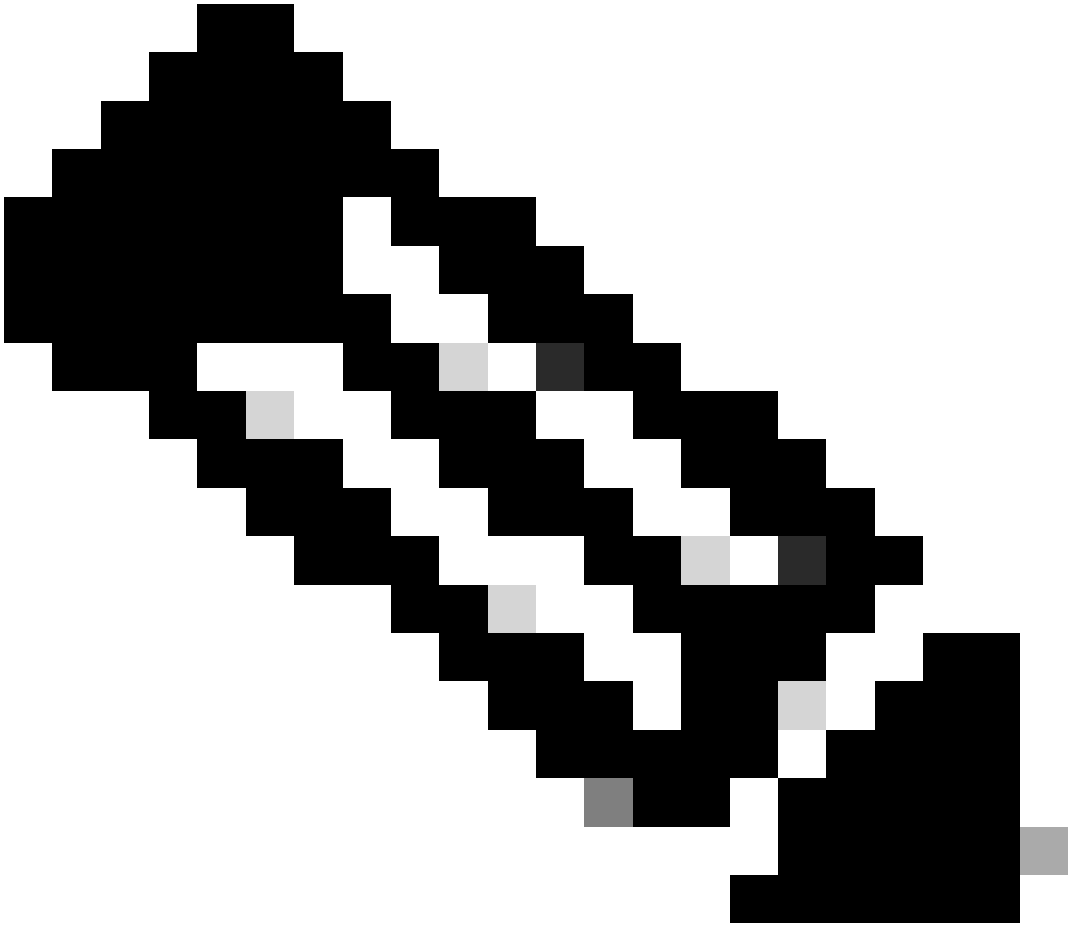
기본 키가 구성되면 라우터 컨피그레이션의 현재 또는 새 키를 암호화하는 데 사용됩니다. 명령줄에 [primary key](기본 키)가 지정되지 않은 경우 라우터는 사용자에게 키를 입력하고 확인을 위해 키를 다시 입력하라는 메시지를 표시합니다. 키가 이미 있는 경우 먼저 기존 키를 입력하라는 메시지가 표시됩니다. password encryption aes 명령을 실행해야 키가 암호화됩니다.

key config-key... 명령을 사용하여 기본 키를 변경할 수 있습니다(어떤 식으로든 키가 손상되지 않

는 한 이 작업은 필요하지 않지만). 새 [primary-key]를 사용하여 다시 명령을 실행합니다.  라우터 컨피그레이션의 현재 암호화된 키는 새 키로 다시 암호화됩니다.

no key config-key를 실행할 때 기본 키를 삭제할 수 있습니다...  그러나 이렇게 하면 라우터 컨피그레이션에서 현재 구성된 모든 키가 쓸모 없게 됩니다(이를 자세히 설명하고 기본 키 삭제를 확인하는 경고 메시지가 표시됨). 기본 키가 더 이상 존재하지 않으므로 유형 6 비밀번호를 해독하여 라우터에서 사용할 수 없습니다.

---



참고: 보안상의 이유로 기본 키를 제거하거나 password encryption 명령을 제거해도 라우터 aes 컨피그레이션의 비밀번호를 해독할 수 없습니다. 비밀번호가 암호화되면 해독되지 않습니다. 기본 키가 제거되지 않은 경우에도 컨피그레이션의 현재 암호화된 키를 계속 해독할 수 있습니다.

---

또한 비밀번호 암호화 기능의 디버그 유형 메시지를 보려면 컨피그레이션 모드에서 **password** logging 명령을 사용합니다.

## 설정

이 문서에서는 라우터에서 다음 구성을 사용합니다.

- 현재 사전 공유 키 암호화
- 대화식으로 새 기본 키 추가
- 현재 기본 키를 대화식으로 수정
- 기본 키 삭제

**현재 사전 공유 키 암호화**

```
<#root>

Router#
```

```
show running-config



Building configuration...
.
.crypto isakmp policy 10
 authentication pre-share
crypto isakmp key cisco123 address 10.1.1.1
.
.
endRouter#



configure terminal



Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#



key config-key password-encrypt testkey123



Router(config)#



password encryption aes



Router(config)#



^Z



Router#
Router#



show running-config
```

```
Building configuration...
.
.
password encryption aes
.
.
crypto isakmp policy 10
 authentication pre-share
crypto isakmp key


6 FLgBaJHXdYY_AcHZZMgQ_RhTDJXHUBAAB


 address 10.1.1.1
.
.
end
```

**대화식으로 새 기본 키 추가**

```
    <#root>

Router(config)#


key config-key password-encrypt


New key:
```

```
<enter key>


Confirm key:


<confirm key>


Router(config)#
```

**현재 기본 키를 대화식으로 수정**

```
    <#root>

Router(config)#


key config-key password-encrypt


 Old key:


<enter current key>


New key:
```

```
<enter new key>



Confirm key:



<confirm new key>



Router(config)#
*Jan  7 01:42:12.299: TYPE6_PASS: Master key change heralded,
re-encrypting the keys with the new primary key
```

**기본 키 삭제**

```
    <#root>

Router(config)#



no key config-key password-encrypt



WARNING: All type 6 encrypted keys will become unusable
Continue with primary key deletion ? [yes/no]:



yes
```

```
Router(config)#
```

## 다음을 확인합니다.

현재 이 설정에 사용 가능한 확인 절차는 없습니다.

## 문제 해결

현재 이 구성에 사용할 수 있는 특정 문제 해결 정보가 없습니다.

## 관련 정보

- **IPsec 지원 페이지**
- **Cisco 기술 지원 및 다운로드**

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.