

# 보안 네트워크 분석에 NTP 인증 구성

## 목차

---

### [소개](#)

#### [사전 요구 사항](#)

##### [요구 사항](#)

##### [사용되는 구성 요소](#)

### [구성](#)

#### [NTP 구성 요구 사항](#)

#### [키값 세부 정보](#)

#### [구성 SNA 관리자 NTP 인증](#)

##### [NTP 서버 설정 열기](#)

##### [NTP 서버 추가](#)

##### [인증 추가](#)

### [다음을 확인합니다.](#)

#### [인증 확인](#)

### [문제 해결](#)

#### [바이트 수 확인](#)

#### [문자 사용 확인](#)

---

## 소개

이 문서에서는 구성된 NTP 서버와의 [연결](#) Secure Network Analytics (SNA) 을 인증하도록 어플라이언스를 구성하는 방법에 대해 설명합니다.

### 사전 요구 사항

### 요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco Secure Network Analytics 어플라이언스 관리
- NTP(Network Time Protocol)

### 사용되는 구성 요소

이 문서에 사용된 Cisco Secure Network Analytics Manager 어플라이언스는 버전 7.4.2입니다.

이 프로세스는 모든 Cisco Secure Network Analytics 어플라이언스 유형에 적용됩니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이

션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

구성

NTP 구성 요구 사항

NTP 통신 인증에 사용되는 값은 다음 요구 사항을 충족해야 합니다.

- 키 ID 값은 65535보다 작거나 같아야 합니다.
- 키 검증은 SHA1입니다
- 키 값은 32자 이하의 인쇄 가능한 영숫자 문자(ASCII)여야 합니다. 0-9, A-Z, a-z 및 기호(단, # 제외)

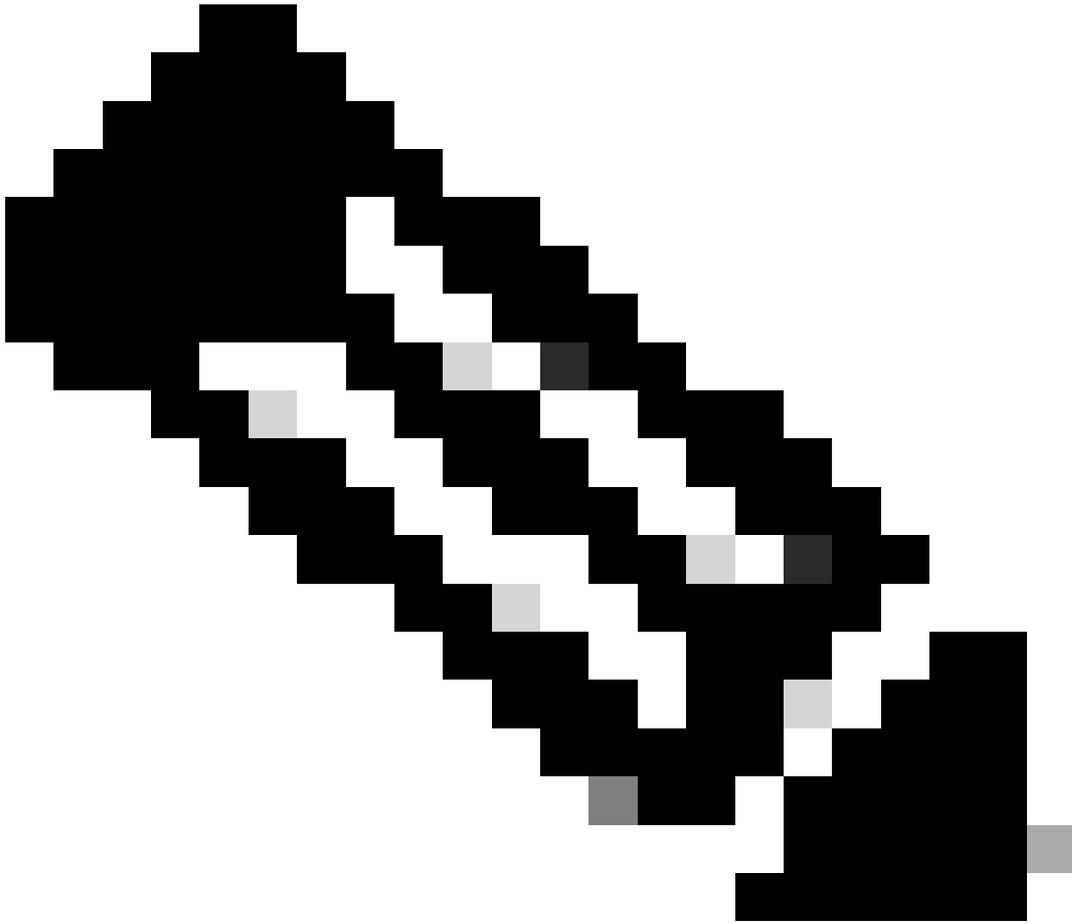
키 값 세부 정보

NTP에서는 20바이트보다 긴 키 값이 16진수로 가정합니다.

Key Value의 최대 길이는 64바이트이므로, 6진수 키를 32바이트를 초과할 수 없습니다.

NTP 서버 및 Secure Network Analytics Appliance에 대한 키 값의 예는 표를 참조하십시오.

키 바이트	NTP 서버 키 값 컨피그레이션	보안 네트워크 분
20바 이트 미만	Lan1cope!	Lan1cope!
20바 이트 에서 32바 이트 사이	4C616E31636F7065214C616E31636F7065214C616E31636F7065214C616E3163	Lan1cope!Lan1c



참고: 표에 사용된 값은 예제일 뿐이며 사용자 환경에서 사용할 권장 값이 아닙니다

---

구성 SNA 관리자 NTP 인증

NTP 서버 설정 열기

에 로그인하고 **SNA Manager** 설정을 **NTP Server** 엽니다.

- 주 메뉴에서 을 선택합니다Configure > GLOBAL Central Management.
- Inventory(인벤토리) 탭에서 어플라이언스의 ... (Ellipsis ) 아이콘을 클릭합니다.

- 를 Edit Appliance Configuration 선택합니다.
- 탭을 Network Services 선택합니다.

#### NTP 서버 추가

필요한 경우 이 지침에 따라 선택한 어플라이언스 컨피그레이션에 NTP 서버를 추가합니다.

- NTP Server(NTP 서버) 섹션에서 을 클릭합니다 Add New.
- 필드에서 NTP Servers 드롭다운 화살표를 클릭합니다. 목록에서 NTP 서버를 선택합니다.
- 서버 이름 또는 IP 주소를 입력합니다.
- 를 Add 클릭합니다.
- 를 Apply Settings 클릭합니다.
- 화면 프롬프트를 수락합니다. 어플라이언스가 자동으로 재부팅됩니다.

#### 인증 추가

이 지침에 따라 선택한 NTP 서버에 대한 연결을 인증할 수 있습니다.

**준비:** NTP 서버 키 ID와 키 값이 있어야 합니다.

- NTP Server 섹션에서 NTP 서버의 ... (Ellipsis) 아이콘을 클릭합니다.
- 를 Authenticate Connection 선택합니다.
- 키 ID 및 키 값을 입력합니다.
- Apply Authentication 을 클릭합니다.
- 를 Apply Settings 클릭합니다.
- 화면 프롬프트를 수락합니다. 어플라이언스가 자동으로 재부팅됩니다.

다음을 확인합니다.

#### 인증 확인

서버에 인증을 추가할 경우 키 아이콘은 인증이 구성되었음을 나타냅니다. 인증 이 성공 확인 하려면 감사 로그를 검토 해야 합니다.

- 주 메뉴에서 을 선택합니다Configure > GLOBAL Central Management.
- Inventory(인벤토리) 탭에서 어플라이언스의 ... (Ellipsis) 아이콘을 클릭합니다.
- 를 Support선택합니다.
- 탭을 Audit Logs 선택합니다.
- 필드에서 Category 을 선택합니다Management.
- 를 Search 클릭합니다.
- NTP 통신 상태 및 시스템 시간 변경이 성공한 것으로 표시되는지 확인합니다. Success(성공) 열을 선택하여 이벤트가 Yes(예)로 표시되는지 확인합니다.

## 문제 해결

### 바이트 수 확인

Linux 디바이스에서 셸을 사용하여 Key Values의 바이트 수를 테스트할 수 있습니다.

예제의 키 값은 이 문서의 키 값 길이 섹션에 있는 테이블에서 가져옵니다.

명령을 `echo -n '{key_value}' | wc -c` 실행하여 {key\_value}을(를) 사용할 키 값으로 대체하는 바이트 수를 확인합니다.

```
742smc:~# echo -n 'Lan1cope!' | wc -c 9 742smc:~# echo -n 'Lan1cope!Lan1cope!Lan1cope!Lan1c' | wc -c 32
```

행 2, 4, 6의 출력은 키 값 바이트 수가 각각 9, 32, 64임을 보여준다.

### 문자 사용 확인

바이트 수가 20보다 작은 경우 NTP 컨피그레이션 요구 사항에 설명된 대로 인쇄 가능한 ASCII 문자를 사용해야 합니다.

명령을 실행하여 `echo '{key_value}' | xxd -r -p && echo` HEX 값을 사용하려는 키 값으로 {key\_value}을(를) 대체하는 ASCII로 변환할 수 있습니다.

```
742smc:~# echo '4C616E31636F7065214C616E31636F7065214C616E31636F7065214C616E3163' | xxd -r -p && echo L
```

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.