

# CLI를 사용하여 Catalyst 1300 Switch에서 Change of Authorization의 기본 구성

## 목표

이 문서의 목적은 CLI(Command Line Interface)를 사용하여 Catalyst 1300 스위치에서 CoA(change of authorization) 기능의 기본 구성을 수행하는 방법을 설명하는 것입니다.

## 적용 가능한 장치 및 소프트웨어 버전

- Catalyst 1300 스위치 | 4.1.3.36

## 소개

CoA(Change of Authorization)는 RADIUS 프로토콜의 확장으로, 인증된 후 AAA(Authentication, Authorization, and Accounting) 또는 dot1x 사용자 세션의 속성을 변경할 수 있습니다. AAA의 사용자 또는 그룹에 대한 정책이 변경되면 관리자는 AAA 서버(예: Cisco ISE)에서 RADIUS CoA 패킷을 전송하여 인증을 다시 초기화하고 새 정책을 적용할 수 있습니다.

Cisco ISE(Identity Services Engine)는 완전한 기능을 갖춘 네트워크 기반 액세스 제어 및 정책 시행 엔진입니다. 보안 분석 및 시행, RADIUS 및 TACACS 서비스, 정책 배포 등을 제공합니다. Cisco ISE는 현재 Catalyst 1300 스위치에 대해 지원되는 유일한 CoA 동적 권한 부여 클라이언트입니다. 자세한 내용은 [ISE 관리 가이드](#)를 참조하십시오.

펌웨어 버전 4.1.3.36의 Catalyst 1300 스위치에 CoA 지원이 추가되었습니다. 여기에는 사용자 연결을 끊고 사용자 세션에 적용할 수 있는 권한 부여를 변경하는 지원이 포함됩니다. 디바이스는 다음 CoA 작업을 지원합니다.

- 세션 연결 끊기
- 호스트 포트 CoA 명령 비활성화
- 바운스 호스트 포트 CoA 명령
- 호스트 CoA 재인증 명령

이 문서에서는 CLI를 사용하는 Catalyst 1300 스위치의 기본 CoA 구성에 대한 명령을 확인할 수 있습니다. 단계는 사용자 설정 및 요구 사항에 따라 달라질 수 있습니다.

## 목차

- [CLI를 사용한 기본 CoA 컨피그레이션](#)

- [CoA 컨피그레이션에 대한 기타 명령](#)
- [권한 Exec 모드의 CLI 명령](#)

## CLI를 사용한 기본 CoA 컨피그레이션

### RADIUS 서버 및 RADIUS 계정 관리 설정

전역 컨피그레이션 모드에서 RADIUS 서버를 구성하려면 다음 명령을 사용합니다.

#### 1단계

디바이스와 RADIUS 데몬 간의 RADIUS 통신을 위한 인증 키를 설정하려면 `radius-server key` 명령을 사용합니다.

```
radius-server key
```

#### 2단계

RADIUS 서버 호스트를 구성하려면 `radius-server host` 명령을 사용합니다.

```
radius-server host key priority 1 usage dot1x
```

- IP 주소는 ISE 서버 IP 주소가 됩니다.
- `key <key-string>` - 디바이스와 RADIUS 서버 간의 모든 RADIUS 통신에 대한 인증 및 암호화 키를 지정합니다. 이 키는 RADIUS 데몬에 사용된 암호화와 일치해야 합니다.
- `Priority` - 서버가 사용되는 순서를 지정합니다. 0의 우선순위가 가장 높습니다. (범위:0-65535)
- `usage dot1x` - RADIUS 서버가 802.1x 포트 인증에 사용되도록 지정합니다.

#### 3단계

```
aaa accounting dot1x start-stop group radius
```

### 동적 권한 부여 서버 구성

#### 1단계

전역 컨피그레이션 모드에서 다음 명령을 실행하여 CoA 컨피그레이션 모드로 들어갑니다.

```
aaa server radius dynamic-author
```

#### 2단계

디바이스와 CoA 클라이언트 간에 공유할 RADIUS 키를 구성하려면(범위: 0-128자), 동적 권한 부여 로컬 서버 컨피그레이션 모드에서 `server-key <key-string>` 명령을 사용합

니다. CoA 요청에 제공된 키가 이 키와 일치해야 합니다.

```
server-key
```

**Note:**

ISE의 경우 key-string은 RADIUS를 구성할 때 RADIUS 서버 key-string에 대해 지정한 키 문자열과 동일합니다.

### 3단계

CoA 클라이언트 호스트 IP 주소를 입력 합니다. IP 주소는 IPv4, IPv6 또는 IPv6z 주소일 수 있습니다.

```
client
```

### 4단계

```
Exit
```

## 802.1x 구성

802.1X를 전역적으로 활성화하려면 dot1x system-auth-control 명령을 사용합니다.

```
dot1x system-auth-control
```

## 포트에 802.1x 구성

### 1단계

인터페이스 컨피그레이션을 입력하고 interface GigabitEthernet<Interface ID> 명령을 사용하여 인터페이스 ID를 선택합니다.

```
interface gil/0/1
```

### 2단계

포트 권한 부여 상태의 수동 제어를 활성화하려면 dot1x port-control 명령을 사용합니다. 자동 모드는 디바이스에서 802.1X 인증을 활성화하고 디바이스와 클라이언트 간의 802.1X 인증 교환을 기반으로 하여 해당 포트가 권한 있는 상태 또는 권한이 없는 상태로 전환되도록 합니다.

```
dot1x port-control auto
```

### 3단계

모든 802.1X 지원 포트 또는 지정된 802.1X 지원 포트의 수동 재인증을 시작하려면 특권 EXEC 모드에서 dot1x re-authenticate 명령을 사용합니다.

```
dot1x re-authenticate gil/0/1
```

### 4단계

포트 보안 학습 모드를 구성하려면 port security mode Interface (Ethernet, Port Channel) 컨피그레이션 모드 명령을 사용합니다. Secure delete-on-reset 매개변수는 delete-on-reset TTL(Time-of-Live)을 사용하는 학습 보안 MAC 주소가 제한된 보안 모드입니다.

```
port security mode secure delete-on-reset
```

### 5단계

인터페이스 컨피그레이션을 종료하려면 다음을 입력합니다.

```
exit
```

## CoA 컨피그레이션에 대한 기타 명령

다음은 컨피그레이션 및 설정에 따라 사용할 수 있는 몇 가지 다른 CoA 명령입니다.

- attribute event-timestamp drop-packet - 이 명령은 동적 권한 부여 로컬 서버 컨피그레이션 모드에서 사용되어 이벤트 타임스탬프 특성을 포함하지 않는 PoD(Packet of Disconnect) 요청 또는 CoA 요청을 삭제하도록 디바이스를 구성합니다.

```
attribute event-timestamp drop-packet
```

- authentication command bounce-port ignore - 디바이스가 RADIUS CoA(Change of Authorization) bounce port 명령을 무시하도록 구성하려면 글로벌 컨피그레이션 모드에서 authentication command bounce-port ignore 명령을 사용합니다.

```
authentication command bounce-port ignore
```

- authentication command disable-port ignore - RADIUS CoA disable-port 명령을 무시하도록 디바이스를 구성하려면 글로벌 컨피그레이션 모드에서 이 명령을 사용합니다.

```
authentication command disable-port ignore
```

- domain delimiter <character> - 수신한 PoD 및 CoA 요청에 대해 사용자 이름 도메인 구분 기호를 구성하려면 동적 권한 부여 로컬 서버 컨피그레이션 모드에서 domain delimiter 명령을 사용합니다.

```
domain delimiter $
```

이 예에서는 \$ 문자가 구분 기호로 구성됩니다.

- domain stripping [right-to-left] - 수신된 PoD 및 CoA 요청에 대해 사용자 이름 도메인 스트리핑에 대한 동작을 활성화하고 정의하려면 동적 권한 부여 로컬 서버 컨피그레이션 모드에서 domain stripping 명령을 사용합니다.

```
domain stripping right-to-left
```

- ignore server-key - 이 명령은 동적 권한 부여 로컬 서버 컨피그레이션 모드에서 CoA 서버 키를 무시하도록 디바이스를 구성하는 데 사용됩니다.

```
ignore server-key
```

## 권한 Exec 모드의 CLI 명령

권한 exec 모드에서 인증된 클라이언트에 대해 show 명령을 실행하고, 클라이언트 카운터를 지우고, 동적 권한 부여 서버 컨피그레이션을 표시할 수 있습니다.

- show aaa clients를 사용하여 AAA(CoA) 클라이언트의 통계를 표시할 수 있습니다.

```
show aaa clients
```

- CoA 컨피그레이션을 표시하려면 show aaa server radius dynamic-author 명령을 사용합니다.

```
show aaa server radius dynamic-author
```

- clear aaa counters를 사용하여 aaa 클라이언트 카운터를 지울 수 있습니다

```
clear aaa clients counters
```

## 결론

이제 CLI를 사용하여 Catalyst 1300 스위치에서 기본 CoA(Change of Authorization) 컨피그레이션을 완료했습니다.

Catalyst 1300 스위치의 CLI 명령에 대한 자세한 내용은 [Cisco Catalyst 1300 스위치 시리즈 CLI 가이드를 참조하십시오](#).

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.