무선 게스트 액세스 FAQ

목차

소개

이 문서에서는 Cisco Unified Wireless 네트워크에 포함되어 있는 무선 게스트 액세스 기능에 대해 자주 묻는 질문(FAQ)에 대한 정보를 제공합니다.

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

안전하지 않은 네트워크 영역에 대한 EoIP(Ethernet over IP) 터널이란 무엇입니까?

Cisco에서는 게스트 트래픽 전용 컨트롤러를 사용할 것을 권장합니다. 이 컨트롤러를 게스트 앵커 컨트롤러라고 합니다.

게스트 앵커 컨트롤러는 일반적으로 DMZ(demilitarized zone)라고 하는 안전하지 않은 네트워크 영역에 있습니다. 트래픽이 시작되는 다른 내부 WLAN 컨트롤러가 엔터프라이즈 LAN에 있습니다. 엔터프라이즈 데이터 트래픽에서 게스트 트래픽의 경로 격리를 보장하기 위해 내부 WLAN 컨트롤러와 게스트 앵커 컨트롤러 간에 EoIP 터널이 설정됩니다. 경로 격리는 게스트 액세스를 위한 중요한 보안 관리 기능입니다. 또한 보안 및 QoS(Quality of Service) 정책을 분리할 수 있으며 게스트 트래픽과 기업 또는 내부 트래픽 간에 차별화됩니다.

Cisco Unified Wireless Network 아키텍처의 중요한 기능은 EoIP 터널을 사용하여 하나 이상의 프로비저닝된 WLAN(즉, SSID)을 네트워크 내의 특정 게스트 앵커 컨트롤러에 정적으로 매핑하는 기능입니다. 매핑된 WLAN을 오가는 모든 트래픽은 원격 컨트롤러와 게스트 앵커 컨트롤러 간에 설정된 고정 EoIP 터널을 통과합니다.

이 기술을 사용하면 모든 관련 게스트 트래픽이 기업 네트워크를 통해 보안되지 않은 네트워크 영역에 있는 게스트 앵커 컨트롤러로 투명하게 전송될 수 있습니다.

게스트 앵커 컨트롤러로 구축할 알맞은 컨트롤러를 선택하려면 어떻게 해야 합니까?

게스트 앵커 컨트롤러를 선택하는 것은 활성 게스트 클라이언트 세션 수에 의해 정의된 게스트 트래픽의 양, 컨트롤러의 업링크 인터페이스 용량에 의해 정의된 게스트 트래픽의 양 또는 둘 모두의 함수입니다.

게스트 앵커 컨트롤러당 총 처리량 및 클라이언트 제한은 다음과 같습니다.

- Cisco 2504 Wireless LAN Controller - 4 * 1Gbps 인터페이스 및 1000개의 게스트 클라이언트
- Cisco 5508 WLC(Wireless LAN Controller) - 8Gbps 및 7,000개의 게스트 클라이언트
- Cisco Catalyst 6500 Series WiSM-2(Wireless Services Module) - 20Gbps 및 15,000개의 클라이언트
- Cisco 8500 WLC(Wireless LAN Controller) - 10Gbps 및 64,000개의 클라이언트

참고: Cisco 7500 WLC는 게스트 앵커 컨트롤러로 구성할 수 없습니다. 게스트 앵커 기능을 지원하는 WLC 목록은 보안되지 않은 네트워크 영역에서 게스트 액세스를 지원하는 데 사용할 수 있는 컨트롤러는 무엇입니까?를 참조하십시오.

각 컨트롤러의 데이터베이스에 최대 2048개의 게스트 사용자 이름 및 비밀번호를 저장할 수 있습니다. 따라서 활성 게스트 자격 증명의 총 수가 이 수를 초과하는 경우 둘 이상의 컨트롤러가 필요합니다. 또는 게스트 자격 증명을 외부 RADIUS 서버에 저장할 수 있습니다.

네트워크의 액세스 포인트 수는 게스트 앵커 컨트롤러 선택에 영향을 미치지 않습니다.

게스트 앵커 컨트롤러에서 종료할 수 있는 EoIP(Ethernet over IP) 터널의 수는 몇 개입니까?

하나의 게스트 앵커 컨트롤러는 내부 WLAN 컨트롤러에서 최대 71개의 EoIP 터널을 종료할 수 있습니다. 이 용량은 WLC- 2504를 제외한 모든 Cisco Wireless LAN Controller 모델에서 동일합니다. 2504 컨트롤러는 최대 15개의 EoIP 터널을 종료할 수 있습니다. 추가 터널이 필요한 경우 둘 이상의 게스트 앵커 컨트롤러를 구성할 수 있습니다.

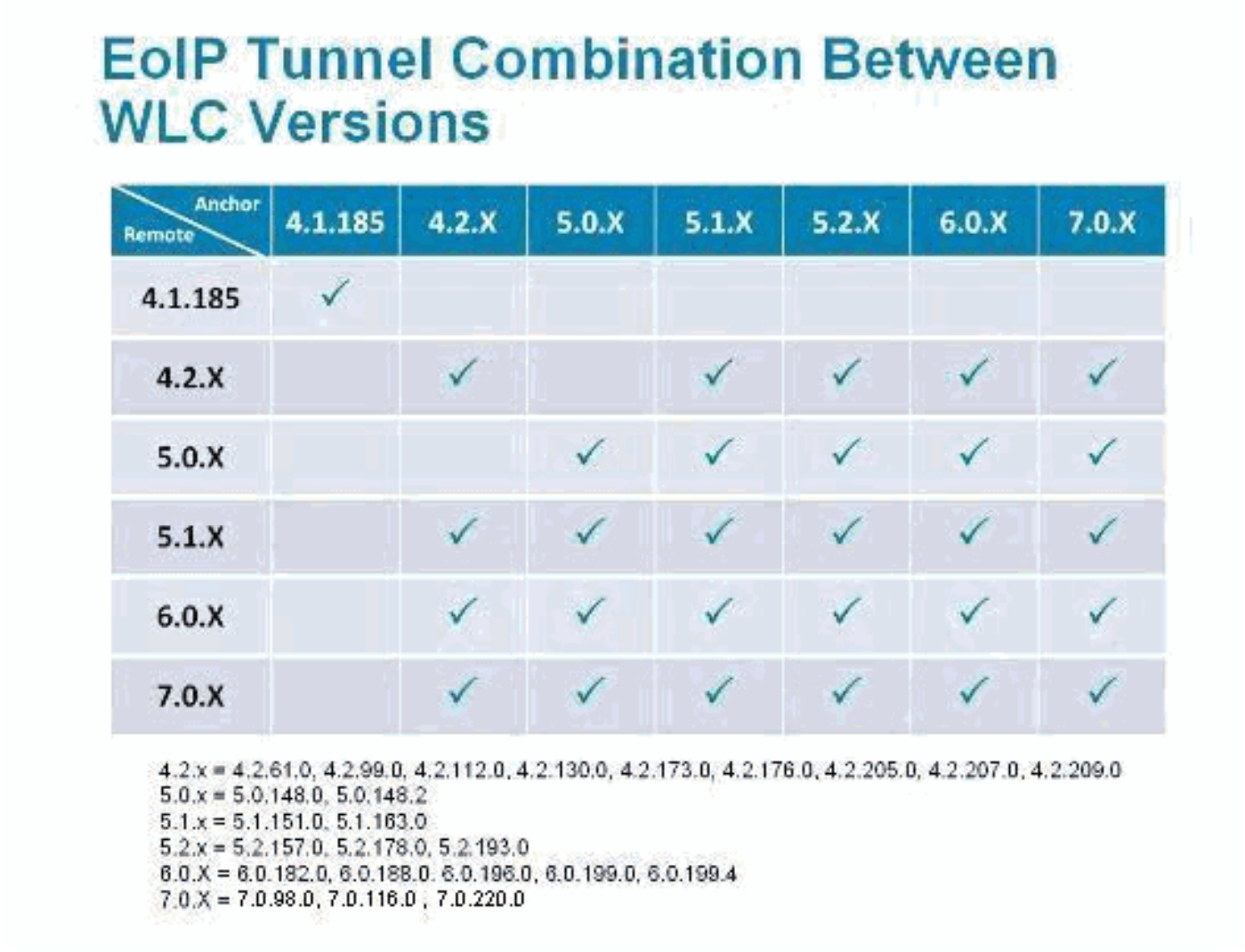
EoIP 터널은 각 EoIP에 있는 터널링된 WLAN 또는 SSID(Secure Set Identifier)의 수와 독립적으로 WLAN 컨트롤러당 계산됩니다.

게스트 앵커 컨트롤러와 게스트 클라이언트 연결을 사용하는 액세스 포인트를 지원하는 각 내부 컨트롤러 간에 하나의 EoIP 터널이 구성됩니다.

서로 다른 소프트웨어 버전을 실행하는 컨트롤러 간에 EoIP(Ethernet over IP) 터널을 생성할 수 있습니까?

일부 Wireless LAN Controller 소프트웨어 버전에서는 이 기능을 지원하지 않습니다. 이러한 경우 원격 및 앵커 컨트롤러는 동일한 버전의 WLC 소프트웨어를 실행해야 합니다. 그러나 최신 소프트웨어 버전에서는 원격 컨트롤러와 앵커 컨트롤러의 버전이 서로 다릅니다.

이 매트릭스는 EoIP 터널을 생성할 수 있는 Wireless LAN Controller 소프트웨어 버전을 나열합니다.



Cisco 2100/2500 Series Wireless LAN Controller를 비보안 네트워크 영역에서 게스트 앵커 컨트롤러로 사용할 수 있습니까?

예, Cisco Unified Wireless Network Software Release 7.4부터 Cisco 2500 Series Wireless LAN Controller는 방화벽 외부의 게스트 트래픽(최대 15개의 EoIP 터널)을 종료할 수 있습니다. Cisco 2000 Series Wireless LAN Controller는 게스트 터널만 생성할 수 있습니다.

Cisco Wireless LAN Controller Module for Integrated Services Routers(WLCM 또는 WLCM2)를 비보안 네트워크 영역에서 게스트 앵커 컨트롤러로 사용할 수 있습니까?

아니요. WLCM 또는 WLCM2는 게스트 터널을 종료할 수 없습니다. WLCM은 게스트 터널만 시작할 수 있습니다.

안전하지 않은 네트워크 영역에서 게스트 액세스를 지원하는 데 어떤 컨트롤러를 사용할 수 있습니까?

게스트 클라이언트의 EoIP 터널 종료, 웹 인증 및 액세스 제어를 포함하는 게스트 터널 앵커 기능은 다음 Cisco Wireless LAN Controller 플랫폼(버전 4.0 이상 소프트웨어 이미지 포함)에서 지원됩니

다.

- Cisco Catalyst 6500 Series WiSM2(Wireless Services Module)
- Cisco WiSM-2 Series Wireless LAN Controller
- Cisco Catalyst 3750G Integrated Wireless LAN Controller
- Cisco 5508 Series Wireless LAN Controller
- Cisco 2500 Series Wireless LAN Controller(소프트웨어 릴리스 7.4에 도입된 지원)

방화벽 외부에서 게스트 앵커 컨트롤러를 사용하는 경우 게스트 액세스를 위해 어떤 방화벽 포트가 열려 있습니까?

게스트 앵커 컨트롤러와 원격 컨트롤러 간의 방화벽에서는 다음 포트를 열어야 합니다.

- 레거시 모빌리티: 사용자 데이터 트래픽용 IP 프로토콜 97, UDP 포트 16666
- 새로운 모빌리티: UDP 포트 16666 및 16667

선택적 관리를 위해 다음과 같은 방화벽 포트를 열어야 합니다.

- SSH/텔넷 - TCP 포트 22/23
- TFTP - UDP 포트 69
- NTP - UDP 포트 123
- SNMP - UDP 포트 161(가져오기 및 설정) 및 162(트랩)
- HTTPS/HTTP - TCP 포트 443/80
- Syslog - TCP 포트 514
- RADIUS 인증/계정 UDP 포트 1812 및 1813

게스트 트래픽이 NAT(Network Address Translation)가 구성된 방화벽을 통과할 수 있습니까?

방화벽을 통과하는 EoIP 터널에서 일대일 NAT를 사용해야 합니다.

Anchor - Foreign WLC 시나리오에서 어떤 WLC가 RADIUS 계정 관리를 전송합니까?

이 시나리오에서 인증은 항상 앵커 WLC에 의해 수행됩니다. 따라서 RADIUS 어카운팅은 앵커 WLC에 의해 전송됩니다.

> **참고**: CWA(Central Web Authentication) 및/또는 CoA(Change of Authorization) 구축에서는 RADIUS 어카운팅이 앵커에서 비활성화되어야 하며 외부 WLC에서만 사용됩니다.

내부 컨트롤러와 앵커 컨트롤러 간의 게스트 터널이 실패합니다. WLC에서 다음 로그를 확인합니다. **mm_listen.c:5373 MM-3-INVALID_PKT_RECVD: 10.40.220.18 . :0.0.0. .. 왜 그럴까요?**

WLANs 페이지의 WLC GUI에서 터널 상태를 **확인할 수** 있습니다. WLAN 옆의 드롭다운 상자를 클

릭하고 제어 및 데이터 **경로**의 상태를 포함하는 Mobility Anchors를 선택합니다. 다음 이유 중 하나로 인해 오류 메시지가 표시됩니다.

1. 앵커 및 내부 컨트롤러가 다른 버전의 코드에 있습니다. 동일한 버전의 코드를 실행해야 합니다.
2. 모빌리티 앵커 컨피그레이션의 컨피그레이션이 잘못되었습니다. DMZ가 자체적으로 모빌리티 앵커로 구성되어 있고 내부 WLC에 DMZ WLC가 모빌리티 앵커로 구성되어 있는지 확인합니다. 모빌리티 앵커를 구성하는 방법에 대한 자세한 내용은 Cisco Wireless LAN Controller 컨피그레이션 가이드, 릴리스 7.0의 Configuring Auto-Anchor Mobility 섹션을 참조하십시오. 그러면 게스트 사용자가 트래픽을 전달할 수 없게 됩니다.

무선 게스트 액세스 설정에서 클라이언트는 DHCP 서버에서 IP 주소를 받지 않습니다. Thu Jan 22 16:39:09 2009: XX:XX:XX:XX:XX:XX DHCP Dropping Reply from Export-Foreign STA 오류 메시지가 내부 컨트롤러에 나타납니다. 왜 그럴까요?

무선 게스트 액세스 설정에서 게스트 앵커 컨트롤러와 내부 컨트롤러의 DHCP 프록시 설정이 일치해야 합니다. 그렇지 않으면 클라이언트의 DHCP 요청이 삭제되고 내부 컨트롤러에 다음과 같은 오류 메시지가 표시됩니다.

```
Thu Jan 22 16:39:09 2009: XX:XX:XX:XX:XX:XX  DHCP dropping REPLY from Export-Foreign STA
```

WLC에서 dhcp 프록시 설정을 변경하려면 다음 명령을 사용합니다.

```
(Cisco Controller) >config dhcp proxy ?

enable          Enable DHCP processing's proxy style behaviour.
disable         Disable DHCP processing's proxy style behaviour.
```

두 컨트롤러에 **동일한** DHCP 프록시 설정이 있는지 확인하려면 두 컨트롤러에서 show dhcp proxy 명령을 사용합니다.

```
(Cisco Controller) >show dhcp proxy

DHCP Proxy Behaviour: enabled

(Cisco Controller) >
```

게스트 트래픽이 안전하지 않은 네트워크 영역으로 터널링되는 경우 게스트 클라이언트는 어디에서 IP 주소를 얻습니까?

게스트 트래픽은 기업 내에서 EoIP를 통해 레이어 3으로 전송됩니다. 따라서 DHCP(Dynamic Host Configuration Protocol) 서비스를 구현할 수 있는 첫 번째 지점은 게스트 앵커 컨트롤러에 로컬로 있거나 게스트 앵커 컨트롤러가 클라이언트 DHCP 요청을 외부 서버로 릴레이할 수 있습니다. 또한 DNS(Domain Name System) 주소 확인이 처리되는 방법입니다.

Cisco Wireless LAN Controller는 게스트 인증을 위한 웹 포털을 지원합니까?

Cisco Wireless LAN Controller, 소프트웨어 버전 3.2 이상은 인증을 위한 게스트 자격 증명을 캡처하고 간단한 브랜딩 기능과 함께 면책조항 및 사용 제한 정책 정보를 표시하는 기능을 제공하는 내장형 웹 포털을 제공합니다.

웹 포털을 사용자 지정하려면 어떻게 해야 합니까?

웹 포털을 사용자 정의하는 방법에 대한 자세한 내용은 웹 인증 로그인 페이지 선택을 참조하십시오.

게스트 자격 증명은 어떻게 관리됩니까?

게스트 자격 증명은 Cisco WCS(Wireless Control System) 버전 7.0 또는 NCS(Network Control System) 버전 1.0을 사용하여 중앙에서 생성 및 관리할 수 있습니다. 네트워크 관리자는 게스트 자격 증명을 만들 목적으로 "로비 앰버서더" 액세스를 허용하는 WCS 내에서 제한된 권한의 관리 계정을 설정할 수 있습니다. WCS 또는 NCS에서 로비 앰버서더 계정을 가진 사용자는 게스트 앵커 컨트롤러 역할을 하는 컨트롤러에 대한 게스트 자격 증명을 생성, 할당, 모니터링 및 삭제할 수 있습니다.

로비 앰버서더는 게스트 사용자 이름(또는 사용자 ID)과 비밀번호를 입력하거나 자격 증명을 자동 생성할 수 있습니다. 또한 모든 게스트에 대해 하나의 사용자 이름 및 비밀번호를 사용하거나 각 게스트에 대해 고유한 사용자 이름 및 비밀번호를 사용할 수 있도록 하는 전역 컨피그레이션 매개변수도 있습니다.

WCS에서 로비 앰버서더 계정을 구성하려면 Cisco Wireless Control System Configuration Guide, Release 7.0의 Creating Guest User Accounts 섹션을 참조하십시오.

WCS(Wireless Control System) 또는 NCS 외에 Cisco Wireless LAN Controller에서도 로비 앰버서더 기능을 사용할 수 있습니까?

예. WCS 또는 NCS가 구축되지 않은 경우 네트워크 관리자는 게스트 앵커 컨트롤러에서 로비 앰배서더 계정을 설정할 수 있습니다. 로비 앰배서더 계정을 사용하여 게스트 앵커 컨트롤러에 로그인하는 사람은 게스트 사용자 관리 기능에만 액세스할 수 있습니다.

여러 게스트 앵커 컨트롤러가 있는 경우 여러 게스트 앵커 컨트롤러에서 사용자 이름을 동시에 구성하려면 WCS 또는 NCS를 사용해야 합니다.

Wireless LAN Controller를 사용하여 로비 앰배서더 계정을 만드는 방법에 대한 자세한 내용은 Cisco Wireless LAN Controller 컨피그레이션 가이드, 릴리스 7.0의 로비 앰배서더 계정 만들기 섹션을 참조하십시오.

게스트는 외부 AAA(authentication, authorization, and accounting) 서버로 인증할 수 있습니까?

예. 게스트 인증 요청은 외부 RADIUS 서버로 릴레이할 수 있습니다.

게스트가 로그온하면 어떻게 됩니까?

무선 게스트가 웹 포털을 통해 로그인하면 게스트 앵커 컨트롤러는 다음 단계를 수행하여 인증을 처리합니다.

1. 게스트 앵커 컨트롤러는 로컬 데이터베이스에서 사용자 이름 및 비밀번호를 확인하고, 해당 데이터베이스가 있는 경우 액세스 권한을 부여합니다.
2. 사용자 자격 증명이 게스트 앵커 컨트롤러에 로컬로 없는 경우 게스트 앵커 컨트롤러는 WLAN 컨피그레이션 설정을 확인하여 외부 RADIUS 서버가 게스트 WLAN에 대해 구성되었는지 확인합니다. 이 경우 컨트롤러는 사용자 이름과 비밀번호로 RADIUS 액세스 요청 패킷을 생성하고 인증을 위해 선택한 RADIUS 서버에 전달합니다.
3. WLAN에 대해 구성된 특정 RADIUS 서버가 없는 경우 컨트롤러는 전역 RADIUS 서버 컨피그레이션 설정을 확인합니다. "네트워크 사용자"를 인증하는 옵션으로 구성된 모든 외부 RADIUS 서버는 게스트 사용자의 자격 증명으로 쿼리됩니다. 그렇지 않은 경우 "네트워크 사용자"를 선택한 서버가 없고 1단계 또는 2단계를 통해 사용자를 인증하지 않은 경우 인증이 실패합니다.

게스트 사용자 인증을 건너뛰고 웹 페이지 면책조항 옵션만 표시할 수 있습니까?

예. 무선 게스트 액세스의 또 다른 구성 옵션은 사용자 인증을 완전히 우회하고 열린 액세스를 허용하는 것입니다. 그러나 액세스 권한을 부여하기 전에 게스트에게 사용 제한 정책 및 고지 사항 페이지를 제공해야 할 수도 있습니다. 이를 위해 웹 정책 통과를 위해 게스트 WLAN을 구성할 수 있습니다. 이 시나리오에서 게스트 사용자는 면책조항 정보가 포함된 웹 포털 페이지로 리디렉션됩니다. 게스트 사용자의 ID를 활성화 하기 위해, 패스스루 모드는 연결 하기 전에 사용자가 이메일 주소를 입력 할 수 있는 옵션도 있습니다.

원격 컨트롤러와 게스트 앵커 컨트롤러가 동일한 모빌리티 그룹에 있어야 합니까?

아니요. 게스트 앵커 컨트롤러와 원격 컨트롤러는 별도의 모빌리티 그룹에 있을 수 있습니다.

게스트 SSID가 두 개 이상인 경우 각 WLAN(SSID)을 고유한 웹 페이지 포털로 연결할 수 있습니까?

예. 단일 또는 다중 WLAN의 모든 게스트 트래픽은 하나의 웹 페이지로 리디렉션됩니다. WLC 버전 4.2 이상부터 각 WLAN은 고유한 웹 포털 페이지로 이동할 수 있습니다. Cisco Wireless LAN Controller 컨피그레이션 가이드, 릴리스 7.0의 Assigning Login, Login Failure, and Logout Pages per WLAN(WLAN당 로그인, 로그인 실패 및 로그아웃 페이지 할당) 섹션을 참조하십시오.

WLC 릴리스 7.0에서 새로운 설정의 기능인 WebAuth on Mac Filter Failure는 무엇입니까?

WLAN에 레이어 2(mac-filter) 및 레이어 3 보안(webauth-on-macfilter-failure)이 모두 구성된 경우 클라이언트가 둘 중 하나가 통과되면 RUN 상태로 전환됩니다. 그리고 레이어 2 보안(mac-filter)에 실패하면 클라이언트는 레이어 3 보안(webauth-on-macfilter-failure)으로 이동합니다.

브라우저가 프록시 서버용으로 구성된 경우 클라이언트가 제대로 작동합니까?

릴리스 7.0 이전 버전에서는 브라우저에 프록시 서버가 구성되어 있을 때 클라이언트가 TCP 연결을 설정할 수 없었습니다. 릴리스 7.0 이후 이 WebAuth 프록시 서버 지원이 추가되고 컨트롤러에서 프록시 서버 IP 주소 및 포트를 구성할 수 있습니다.

무선 게스트 액세스를 위한 구축 가이드가 있습니까?

구축 가이드의 링크입니다.

구축 설명서: Cisco Wireless LAN Controller를 사용한 Cisco 게스트 액세스

유무선 게스트 액세스를 위한 설계 가이드가 있습니까?

다음은 설계 가이드에 대한 링크입니다.

- Cisco Unified Wireless Guest Access Services
- Cisco WLAN 컨트롤러를 사용한 유선 게스트 액세스 컨피그레이션 예

관련 정보

- **Cisco WLAN 컨트롤러를 사용한 유선 게스트 액세스 컨피그레이션 예**
- **구축 설명서: Cisco Wireless LAN Controller를 사용한 Cisco 게스트 액세스, 릴리스 4.1**
- **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.