

Cisco ISE 엔터프라이즈 및 보안 - 게스트 액세스 관리 v2



마지막 업데이트: 2019 년 7 월 08 일

본 데모에 대하여

본 데모 가이드에는 아래의 내용을 포함합니다:

[본 데모에 대하여](#)

[필요사항](#)

[솔루션 소개](#)

[구성도](#)

[시작하기](#)

[시나리오 1. 핫스팟을 통한 게스트 인터넷 액세스](#)

[시나리오 2. 스폰서 승인을 통한 자체 등록 게스트 액세스](#)

[시나리오 3. 스폰서 게스트 액세스](#)

[What's Next?](#)

필요사항

아래 항목은 데모를 진행하는데 필요한 구성요소입니다.

필수	세부 정보
기본 엔드포인트 라우터	<p>dCloud 에 대해 등록 및 구성된 dCloud 엔드포인트 라우터 키트 (예: 819HWD 라우터)</p> <p>참고: 내부 AP 는 이 데모에서는 작동하지 않으므로 비활성화해야 합니다.</p>
액세스 포인트	<p>엔드포인트 라우터와 함께 사용하기를 선호하지만 사용하지 않고도 가능합니다. 자세한 내용은 이 페이지를 참조하십시오.</p> <p>C9800-CL 에 대해 무선 액세스 지점 지원</p> <p>Cisco AnyConnect®가 장착된 노트북</p>
모니터링 워크스테이션	<p>태블릿, 또는 스마트폰 또는 추가 노트북</p>
사용자 장치	<p>참고: 최상의 경험을 위해 iOS 디바이스를 사용하십시오.</p> <p>Android 도 작동하지만 BYOD 온보딩용 iOS 디바이스 만큼 원활하지 않습니다.</p> <p>참고: 이 데모에서 BYOD 온보딩은 MAC OSX, Windows, Android 및 Apple iOS 에서만 지원됩니다.</p>

참고: 이 데모에는 최소 두 개 이상의 최종 사용자 장치가 있어야 합니다. 백엔드 구성 요소에 모니터링 및 연결하기 위한 최종 사용자 장치 1 개 그리고 온보딩을 위한 최소 1 개의 최종 사용자 장치를 필요합니다.

가치 제안: 데모 중에 랩톱을 온보딩할 계획이라면 두개의 랩톱을 가지고 있어야 합니다. 첫 번째 랩톱은 VPN 옵션을 직접 사용하여 RDP 또는 구성 요소 포털을 통해 dCloud Workstation1 에 액세스하기 위해 필수적이며, 두 번째 랩톱은 핫스팟 또는 게스트 네트워크에 참여하는 것을 시연하기 위해 필요합니다.

참고: AP 및 실제 클라이언트 엔드포인트 디바이스가 없이 게스트를 시연합니다. 관련 게스트 포털의 포털 테스트 URL 을 사용하여 AP 또는 클라이언트 엔드포인트 없이 게스트 플로우를 통과할 수 있습니다. 자세한 내용은 각 섹션에서도 설명합니다.

참고: 최상의 사용자 경험과 데모를 위해 AP 를 실제 클라이언트와 함께 사용하는 것이 권장합니다. RADIUS 라이브 로그와 게스트 보고서는 RADIUS 세션이 없기 때문에 정보가 제한됩니다. 무선 세션이 실제 클라이언트를 리디렉션하는 데 필요하기 때문에 성공한 플로우는 정적 또는 원본 URL 로 보낼 수 없습니다.

솔루션 소개

본 가이드는 무선 기술과 함께 Cisco ISE (Identity Services Engine)를 사용한 여러 Cisco 게스트 액세스 솔루션을 데모하는 데 도움이 됩니다.

ISE 2.2 부터 ISE 는 모든 게스트 플로우에 대해 Apple Mini-Browser (Captive Network Assistant)를 지원합니다. Mini-Browser 는 BYOD 프로우에서도 지원됩니다(몇 가지 알려진 문제 포함).

게스트 및 BYOD 플로우에서 Mini-Browser 를 탐색하려면 다음을 권장합니다:

- dcloud-핫스팟 네트워크에서, 이 브라우저가 자동으로 팝업되도록 WLC 에서 캡티브 포털 바이패스를 비활성합니다.
- dcloud-guest 네트워크(등록, 스폰서드 게스트 및 BYOD 시나리오에서 사용)에서는 캡티브 포털 바이패스를 활성화합니다. 이는 미니 브라우저를 억제하고 팝업하지 않도록 합니다. 또한 디바이스 온보딩을 통과하는 모든 비게스트가 플로우를 성공적으로 완료하지 못하게 합니다.

미니 브라우저를 사용한 자격 증명된 게스트 플로우를 쇼케이스하려면 다음 링크에 있는 명령들을 사용하여 dcloud-guest 네트워크에서 캡티브 포털 바이패스를 비활성화하십시오.

노트: BYOD 시나리오를 사용하기로 결정한 경우 이 설정은 뒤바뀌어야 합니다.

- [Configuring Captive Network Assistant Bypass per WLAN \(GUI\)](#)
- [Configuring Captive Network Assistant Bypass per WLAN \(CLI\)](#)

서포트에 대한 자세한 내용은 다음을 참조하십시오:

- [ISE 2.2 Apple CNA \(Captive Network Assistant\) Mini-Browser for BYOD/Guest](#)
- [Dealing with Apple CNA \(AKA Mini browser\) for ISE BYOD](#)
- [Dual SSID BYOD with Apple Captive Network Assistant \(CNA\) Browser - ISE 2.2](#)

노트: 장치에 리다이렉트 플로우 문제가 있는 경우, [dCloud ISE Demos - Known Caveats](#) 를 참조하십시오.

구성도

본 데모는 시나리오의 원활한 진행 및 솔루션이 제공하는 각 기능들의 동작 확인을 위해 사전 설정된 구성요소들을 포함하고 있습니다. 대부분의 구성요소들은 별도 제공되는 관리자 계정을 통해 설정이 가능하며 **토폴로지** 메뉴에 있는 구성요소 아이콘을 클릭하면 해당 구성요소에 접근하기 위한 IP 어드레스 및 계정 정보를 확인할 수 있습니다.

그림 1: dCloud 구성도

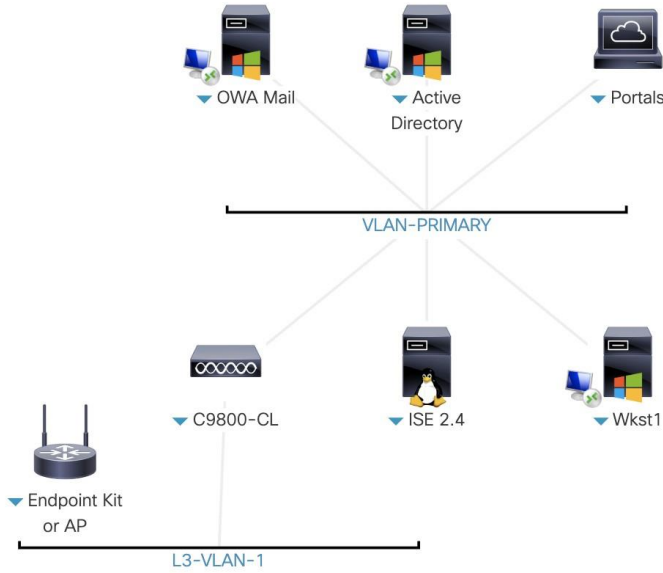


표 1: 장비 세부 사항

장치	IP 주소	액세스 방법	사용자 이름	패스워드	장치
C9800-CL	프라이빗: 198.19.11.10	Workstation1 브라우저	세션 소유자	세션 ID	Wlc.dcloud.cisco.com
	퍼블릭: 세션 세부 사항 참조	로컬 브라우저			
WKST1	198.18.133.36	WebRDP 또는 AnyConnect	administrator	C1sco12345	Workstation1 (RDP access)
	198.18.133.2	WebRDP 또는 AnyConnect	administrator	C1sco12345	OWA Mail - 북마크를 통한 액세스
	198.18.133.1	WebRDP 또는 AnyConnect	administrator	C1sco12345	AD1 (RDP access)
Exchange 서버	198.18.133.110	Putty	linuxuser	C1sco12345	테이블 3 포털을 참조
AD1	198.18.133.27	Workstation1 브라우저	admin	C1sco12345	lse.securitydemo.net

표 3: 사용 가능한 포털

시나리오/ Vertical	메인 포털 URL	스폰서 포털 URL
디폴트/ dCloud	N/A	http://sponsor.securitydemo.net

헬스케어	http://health.dcloud.cisco.com	http://sponsor-health.securitydemo.net
교육	http://edu.dcloud.cisco.com	http://sponsor-edu.securitydemo.net
연방	http://federal.dcloud.cisco.com	http://sponsor-fed.securitydemo.net
기업	http://corp.dcloud.cisco.com	http://sponsor-corp.securitydemo.net

자격 및 액세스 레벨

시나리오 / Vertical	Username	Password	Access Level
헬스케어	의사	C1sco12345	Tier 1 - 전체 액세스
헬스케어	간호사	C1sco12345	Tier 2 - 제한된 액세스
교육	학장	C1sco12345	Tier 1 - 전체 액세스
교육	교수	C1sco12345	Tier 2 - 제한된 액세스
연방	선장	C1sco12345	Tier 1 - 전체 액세스
연방	장교	C1sco12345	Tier 2 - 제한된 액세스
기업	관리자	C1sco12345	Tier 1 - 전체 액세스
기업	종업원	C1sco12345	Tier 2 - 제한된 액세스

데모 시작하기

시작하기에 앞서

고객 및 파트너를 대상으로 데모시연을 할 경우 원활한 진행을 위해 본 자료를 가지고 사전에 충분한 연습을 하시기를 권장합니다. 데모 완료 후 새로운 구성을 해야 하는 경우는 세션을 새로 예약하십시오.

사전에 충분한 연습은 성공적 진행을 위한 필수 조건입니다.

다음 단계에 따라 세션을 예약하고 프레젠테이션 환경을 설정하시기 바랍니다.

1. dCloud 세션 시작합니다. [\[가이드\]](#)

노트: 세션 예약 후 시나리오의 랩이 활성화 되기까지 최대 10 분이 소요될 수 있습니다.

1. 최상의 성능을 위해 랩톱에서 Cisco AnyConnect VPN [\[가이드\]](#) 및 로컬 RDP 클라이언트 [\[가이드\]](#)를 통해 워크스테이션에 연결합니다.

- 워크스테이션 1: **198.18.133.36**, 사용자 이름: **administrator**, 패스워드: **C1sco12345**

노트: Cisco dCloud 원격 데스크톱 클라이언트를 사용하여 워크스테이션에 연결할 수도 있습니다. [\[가이드\]](#). dCloud 원격 데스크톱 클라이언트는 최소한의 상호 작용으로 활성 세션에 액세스하는 데 가장 적합합니다. 그러나 많은 사용자가 이 방법에 대해 연결 및 성능 문제를 경험합니다.

3. **Workstation1** 에서 Firefox 를 엽니다. 고객의 홈페이지는 토폴로지와 백엔드 데모 구성요소에 대한 링크를 볼 수 있는 <http://topo.dcloud.cisco.com> 으로 설정되어 있습니다. 토폴로지 화면으로 돌아가려면 Firefox 에서 홈 버튼을 클릭합니다.

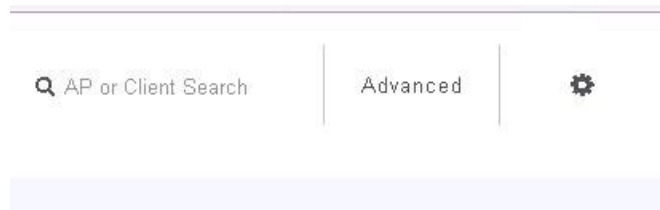
4. Workstation1 에서 데모 WLC(Wireless Controller)에서 Country 를 활성화되어 있는지 확인합니다. [\[가이드\]](#)

노트: 이 데모의 WLC 로그인에는 **세션별 자격 증명**이 필요합니다. **사용자 이름**은 dCloud UI 에 로그인할 때 사용하는 이름이며 **패스워드**는 세션 ID 입니다. 이 정보는 활성 데모의 **세션 세부 정보** 섹션을 참조할 수 있습니다. 또한 **dcloud** 의 일반 사용자 이름이 제공되며, 필요에 따라 고유한 세션 ID 를 패스워드로 사용할 수 있습니다.

5. **호환되는** AP 를 프로비저닝합니다. [\[가이드\]](#)

노트: 엔드포인트 라우터를 사용하는 경우, 이 단계는 한 번만 완료하면 됩니다. 이 데모를 사용할 때 **강력히 권장합니다.** 엔드포인트 라우터가 없는 경우, 새로운 데모를 **예약할 때마다** AP 는 새로운 데모 WLC IP 주소로 재프로비저닝해야 합니다.

6. 오른쪽 상단에서 **Advanced** 를 클릭합니다.



7. AP 가 작동하는지 확인합니다. [\[가이드\]](#)

- 이제 AP 를 통해 **Workstation1** 에 연결할 수 있습니다. [\[가이드\]](#)

8. 데모 위치에 따라 다음과 같은 추가 데모 준비 작업을 완료해야 할 수도 있습니다.

- **시스코 사무실에서 데모하기** 위한 추가 데모 준비 작업을 완료해야 합니다. [\[가이드\]](#)
- **고객 사이트에서 데모하기** 위한 추가 데모 준비 작업을 완료해야 합니다. [\[가이드\]](#)

시나리오 1. 핫스팟을 통한 게스트 인터넷 액세스

가치 제안: 이 시나리오에서 조직은 게스트 인터넷 전용 액세스 권한을 부여해야 하지만, 게스트가 BYOD 온보딩, 스폰서 게스트 액세스 또는 자체 등록 게스트 액세스와 같은 보다 복잡한 단계를 수행하기를 원하지 않습니다. 예를 들어, 카페나 호텔은 게스트에게 핫스팟 인터넷 액세스를 제공하기를 원할 수 있지만, 게스트가 등록 프로세스를 수행하기를 원하지는 않습니다. 이제 Cisco ISE 는 게스트 인터넷 액세스 얻을 수 있는 절차를 단순화해줄 수 있는 핫스팟 게스트 액세스 포털을 제공합니다. 이 시나리오에서는 최종 사용자 디바이스를 사용하여 핫스팟 무선 네트워크에 접속하고 장치가 인터넷 액세스 권한과 *사용 가능한 포털 테이블에* 나열된 기본 수직 포털 페이지에 액세스할 수 있음을 보여줍니다.

스텝

인터넷 핫스팟 액세스

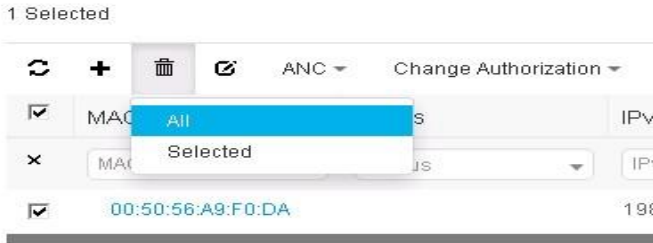
1. 데모에 사용된 각 개인 **유저 BYOD** 디바이스에 대한 설정을 **삭제합니다**. 디바이스 설정이 지워지지 않으면 필요할 때 게스트 포털 또는 다른 페이지로 리디렉션되지 않을 수 있습니다.
 - a. 웹 캐시 삭제 [\[가이드\]](#)
 - b. 개인 장치 설정 삭제 [\[가이드\]](#)

Cisco ISE 엔터프라이즈 및 보안 데모 완료 - 디바이스 온보딩 및 관리 v1

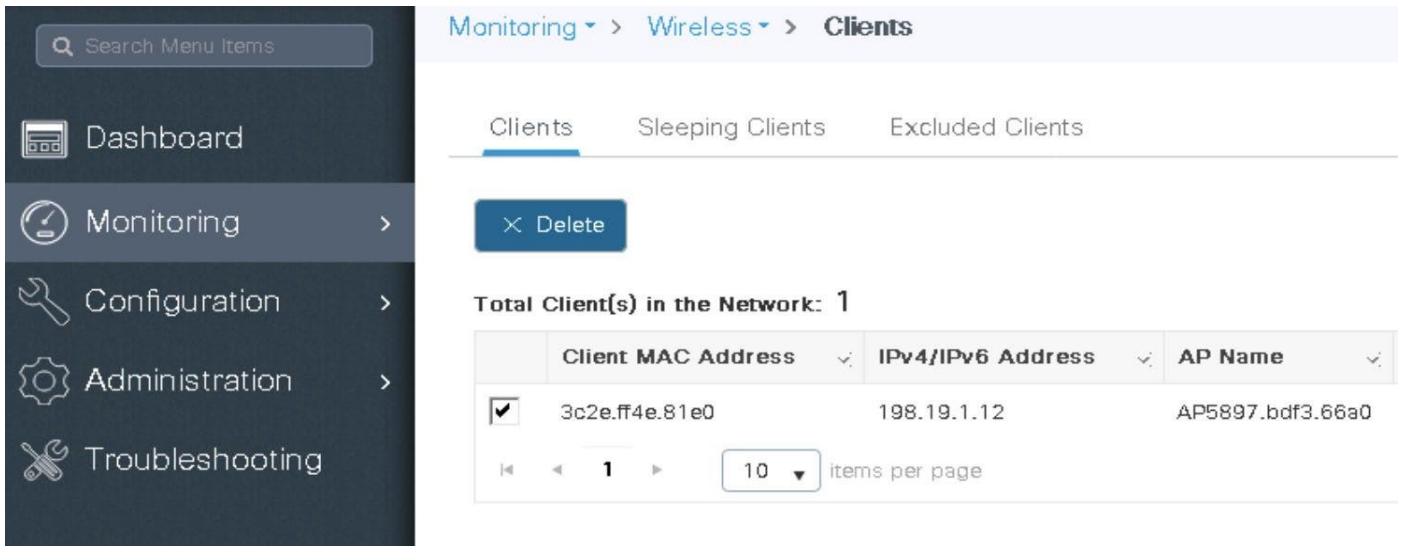
노트: Cisco ISE Enterprise & Security Demo - Device Onboarding and Management v1 을 이미 완료한 경우 다음 단계를 수행하십시오. 이 가이드를 아직 완료하지 않은 경우 아래의 '**Have not Completed the Cisco ISE Enterprise & Security Demo - Device Onboarding and Management v1**'의 하위 섹션으로 건너뛰십시오.

2. **Workstation1** 에서 Firefox 를 열고 <https://ise.securitydemo.net> 유저 ID/패스워드를 **admin/C1sco12345** 조합으로 채우고 다음 방법 중 하나를 사용하여 ISE 에 로그인하십시오:
 - 주소 표시줄에 URL 을 수동으로 입력합니다.
 - 토폴로지 툴바에서 ISE 아이콘을 클릭합니다.
 - 북마크 툴바에서 ISE 북마크에 액세스합니다.
3. 컨텍스트 가시성(Context Visibility)> 엔드포인트(Endpoints)로 이동합니다.
4. 모든 엔드 포인트를 확인하고 삭제합니다.

노트: 만약 엔드포인트 삭제에 문제가 발생하면 브라우저 캐시를 지우고 다시 시도하십시오.



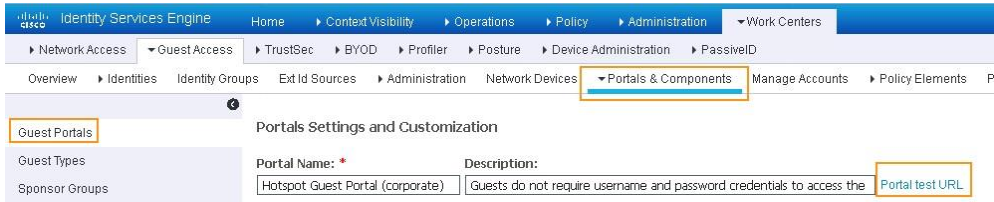
5. Workstation1 에서 다음 방법 중 하나를 사용하여 <http://wlc1.dcloud.cisco.com> 에서 새 탭을 열고 WLC 로그인 페이지에 액세스하십시오:
 - 주소 표시줄에 URL 을 수동으로 입력합니다.
 - 북마크 톨바에 **WLC-9800-CL** 에 대한 북마크를 클릭합니다.
 - 브라우저에서 홈 버튼을 클릭하여 토폴로지 다이어그램으로 돌아가서 vWLC 를 클릭합니다.
7. **MONITOR** 를 클릭합니다.
8. **Clients** 를 클릭합니다.
9. 클라이언트 옆의 확인란을 선택한 다음 **Delete** 를 클릭합니다.
10. **Yes** 를 클릭합니다.



AP 및 실제 클라이언트 엔드포인트 디바이스 없는 게스트 시연

노트: 관련 게스트 포털의 포털 테스트 URL 을 사용하여 AP 또는 클라이언트 엔드포인트 없이 게스트 플로우를 통과할 수 있습니다. 그러나, 최상의 사용자 경험과 데모를 위해 실제 클라이언트와 함께 AP 를 사용하는 것이 권장합니다. RADIUS 라이브 로그 및 게스트 보고서는 RADIUS 세션이 없기 때문에 정보가 제한됩니다. 또한 실제 클라이언트를 리디렉션하는 데 필요한 무선 세션이 있기 때문에 성공 플로우의 정적 또는 원본 URL 로 보낼 수 없습니다.

6. 모니터링 시스템 브라우저 또는 dCloud Workstation 을 사용하여 ISE 포털로 이동합니다.
7. Work Center > Guest Access > Portals & Component 로 이동합니다.
8. (수직 사용자 지정 요구사항에 따라) 원하는 **Hotspot portal** 을 클릭합니다.
9. **Portal test URL link** 를 클릭합니다. 그렇게 하면 포털이 다른 창에 열립니다.



10. 이제, 다음 단계를 수행하고 실제 장치에 적용되는 정보를 건너뛰면서 쿼크 핫스팟 플로우를 수행할 수 있습니다. 정보 중 일부는 적용되지 않은 것을 유의하십시오. 보고 정보도 제한됩니다. 또한 전체 액세스 권한이 있는 시스템에서 포털을 사용하기 때문에 네트워크 리소스에 대한 제한된 액세스를 시연할 수도 없습니다. 시뮬레이션된 플로우이므로 액세스 제어가 적용되지 않습니다.
11. 개인 **User BYOD Device** 를 개방형 네트워크 SSID: **dCloud-Hotspot** 에 연결합니다.

노트: 데모 전체에서 특정 dCloud WiFi 신호에 연결됩니다. 일반적으로는 **DCloud-Hotspot-123456** 과 같은 고유한 세션 ID 가 추가됩니다.

인터넷 핫스팟에 액세스

1. 자동으로 열리지 않으면 사용자 장치에 대해 지원되는 내장된 웹 브라우저를 열고 **HTTP** 를 사용하여 웹 페이지를 검색합니다. **http://enroll.cisco.com** 을 사용하는 것을 권장합니다.

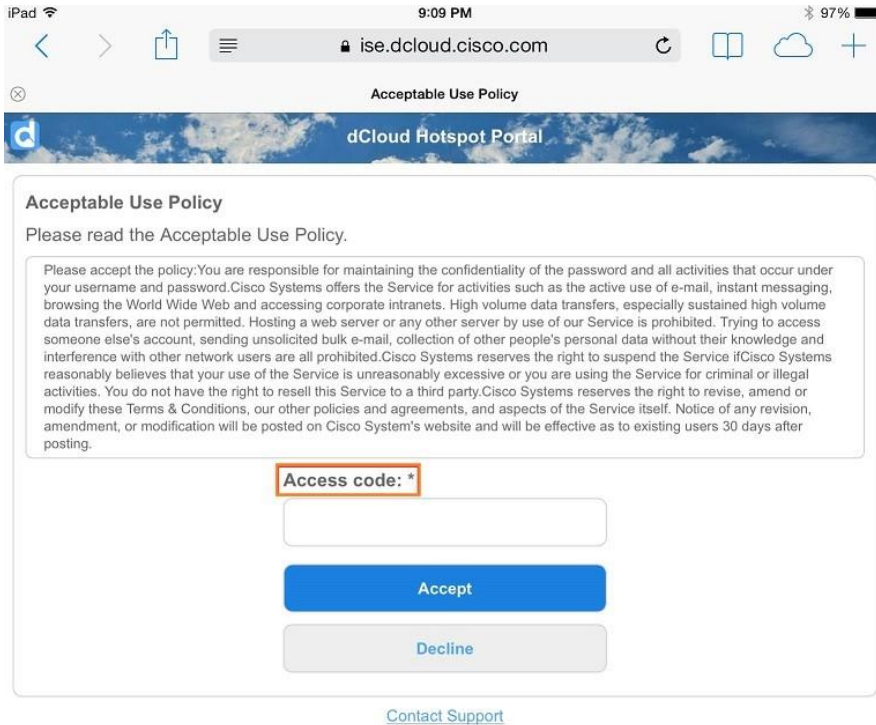
노트: Android 및 브라우저를 사용하여 자동으로 실행되고 문제가 있는 경우, Chrome 을 수동으로 시작합니다.

- 지원되는 브라우저: Apple 디바이스 (Safari), Windows 디바이스 (IE / EDGE, FF / Chrome), Android 디바이스 (Chrome). 전체 자세한 목록은 [Cisco Identity Services Engine 네트워크 구성 요소 호환성, Release 2.4](#) 를 참조하십시오.

노트: 브라우저를 열 때 HTTP 를 사용하여 페이지에 액세스하는 것이 유의하십시오. 만약 HTTPS 를 사용하여 페이지에 액세스하려고 하면 핫스팟 포털로 리디렉션되지 않습니다. 대부분의 최신 운영 체제는 자동 브라우저 시작을 트리거해야 하지만 수동 개입이 필요할 수 있습니다. 고유한 문제로 인해 리디렉션되는 https 는 지원하지 않습니다. [ISE Guest CWA 및 HTTPS 리디렉션을 참조하십시오](#) 를 참조하십시오.

2. 시큐리티 창이 나타나면 **Continue** 를 클릭합니다. 그러면 **dcloud Hotspot Portal** 로 리디렉션되며, 여기에서 **acceptable use policy** 가 제시되고 필요한 **Access Code** 를 입력하라는 메시지가 표시됩니다.

그림: dCloud 핫스팟 포털

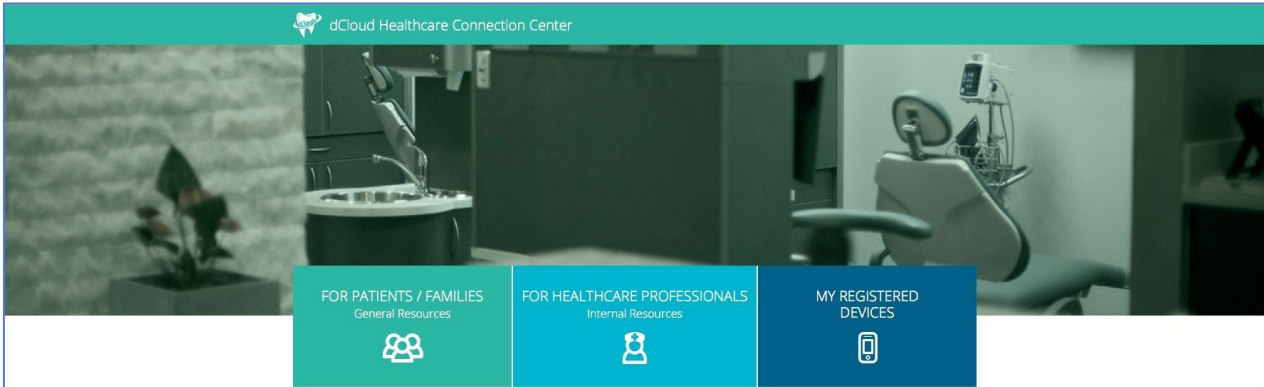


노트: 핫스팟에 대한 액세스 코드를 요구하는 것은 ISE의 선택적 구성입니다. 일부 조직에서는 코드를 입력할 필요 없이 완전히 개방된 인터넷 핫스팟 액세스를 제공하려고 하는 반면, 다른 조직에서는 액세스 코드가 필요한 기본 보안을 선호할 수 있습니다.

노트: 액세스 코드는 핫스팟, 자체 등록 및 인증된 로그인 페이지에서 사용할 수 있습니다. 등록 절차를 거치고 소유자의 동의 없이 서비스를 이용하는 행인으로부터 (예를 들어 주차장이나 같은 건물에 있는 다른 입주자 사무실에 있는 사람들) 게스트 네트워크를 보호하는 데 사용됩니다. 이것은 WPA-PSK SSID 제공의 대안입니다. ISE는 유연하며 고객 요구 사항에 따라 모든 구축에 맞게 구성할 수 있습니다.

3. **Access Code** 를 **dcloud** 에 입력하고 **Accept** 를 클릭합니다. 이 액세스 코드는 대소 문자를 구분합니다.
4. **acceptable use policy** 를 수락한 후 **ISE** 는 네트워크에서 엔드포인트 장치를 다시 인증하는 **COA** 를 전송합니다. 장치가 자동으로 다시 연결되고 <http://www.cisco.com> 으로 리디렉션되어 추가 로그인 자격 증명없이 인터넷에 액세스할 수 있습니다. 이 작업은 최대 30 초가 소요될 수 있습니다.
5. 선택한 시나리오(Healthcare, Education, Federal 또는 Corporate)에 대한 **Main Portal URL**(사용 가능한 포털 테이블에 표시)로 이동합니다. 보안 경고가 발생하면 **Continue** 를 클릭합니다.
6. **General Resources** 를 선택하여 이제 사용자에게 일반 리소스 페이지에 대한 액세스 권한이 있음을 보여줍니다.
7. **Internal Resources** 또는 **My Registered Devices** 를 선택하여 사용자가 이러한 페이지에 액세스하는 것이 제한되어 있음을 보여줍니다.

dCloud 헬스케어 컨넥션 센터 - <http://health.dcloud.cisco.com>



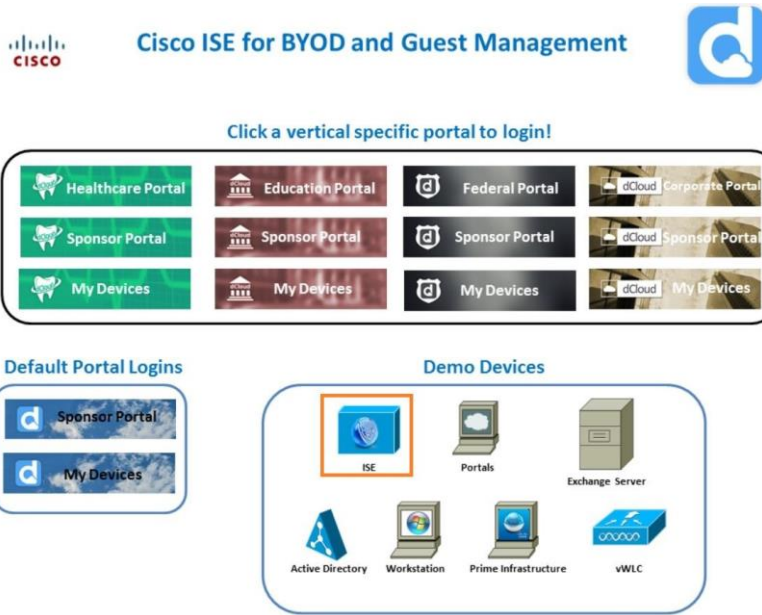
ISE 의 기본 핫스팟 플로우 시연

이제 장치가 핫스팟에 성공적으로 연결하여 인터넷 액세스를 허용했습니다.

다음으로, ISE UI 에 대해 간략하게 살펴보고, 다음과 같은 ISE 의 기본 원리를 어떻게 수행하는지를 보여드리겠습니다:

- 동적으로 디바이스 프로파일링
 - 적절한 인증 프로필 적용; 및
 - 동적으로 허용되는 게스트 인터넷 액세스
1. **Workstation1** 에서 Firefox 를 열고, 다음 방법 중 하나를 사용하고 **admin/C1sco12345** 의 유저 ID/ 비밀번호 조합을 사용하여 <https://ise.securitydemo.net> 에서 ISE 에 로그인합니다.
 - 주소 표시줄에 URL 을 수동으로 입력
 - 토폴로지 툴바에서 ISE 아이콘을 클릭
 - 북마크 툴바에서 ISE 북마크에 액세스

데모 토폴로지 홈페이지: <http://topo.dcloud.cisco.com>



2. 마우스를 **Operations** 메뉴 위에 올려 **RADIUS > Live log** 를 클릭합니다. 이 화면에는 ISE 의 최근 인증 및 권한 부여 시도가 표시됩니다.

노트: 이런 특정한 경우에는 MacBook 이 핫스팟에 연결합니다.

노트: 장치가 처음 dCloud-Hotspot SSID 에 접속하면 MAB(MAC authentication bypass)를 사용하여 인증되고 ISE 는 **HOTSPOT_REDIRECT** 프로파일을 WLC 에 반환합니다. 이는 WLC 에 **모든 사용자 웹 트래픽(all user web traffic)**을 **dCloud Hotspot Portal** 로 리디렉션하도록 지시합니다.

노트: ISE 는 장치를 Apple-iPad 로 올바르게 프로파일링합니다. (이 데모에서는 *장치 유형 기능에 따라 차별화된 액세스*가 표시되지 않습니다.)

노트: 사용자가 올바른 액세스 코드를 입력하고 **acceptable use policy** 를 수락하면 ISE 는 엔드포인트를 재인증하고 **HOTSPOT_ACCESS** 라는 프로파일을 동적으로 할당하는 COA 를 전송합니다. 이 프로파일은 인터넷 및 기본 포털에만 액세스할 수 있도록 WLC 에 미리 구성된 ACL 이름을 푸시합니다.

그림: ISE 는 장치를 Apple-iPad 로 프로파일링하고 핫스팟 액세스를 동적으로 적용합니다.

Status	Details	Identity	Endpoint ID	Authentication Policy	Endpoint Profile	Authorization Policy	Authorization Profiles
		Identity	Endpoint ID	Authentication Policy	Endpoint Profile	Authorization Policy	Authorization Profiles
✓		DC:A4:CA:D2:5F:9D	DC:A4:CAD2:5F:9D	Guest Access	Apple-iPad	Guest Access >> Hotspot Access	HOTSPOT_ACCESS
✓			DC:A4:CAD2:5F:9D				
✓		DC:A4:CA:D2:5F:9D	DC:A4:CAD2:5F:9D	Guest Access >> MAB		Guest Access >> Hotspot Redirect	HOTSPOT_REDIRECT

시나리오 2. 스폰서 승인을 통한 자체 등록된 게스트 액세스

가치 제안: 이 시나리오에서 조직은 방문자를 위해 네트워크에 대한 유연한 게스트 액세스를 제공하고자 합니다. 조직은 게스트가 자신의 게스트 계정을 등록할 수 있는 유연성을 제공하기를 원하지만 사용자가 네트워크에 액세스하기 전에 스폰서가 요청한 계정을 승인하도록 요구하는 추가 보안 및 조직을 원합니다.

이러한 유형의 시나리오에서 사용자는 스폰서가 자신의 모바일 장치에서 게스트 계정을 얻기 위해 필요한 정보를 작성할 수 있으며, 시스템은 스폰서에게 요청을 승인하도록 요청하는 이메일을 보낼 것입니다. 그런 다음 스폰서는 ISE 스폰서 포털에 로그인하여 요청을 승인하거나 거부할 수 있습니다. 스폰서가 계정 요청을 승인하면, ISE 는 사용자 계정을 생성하고 게스트 로그인 자격 증명으로 게스트 사용자에게 이메일 및 SMS 텍스트 메시지를 보냅니다. 그런 다음 게스트는 자격 증명을 사용하여 게스트 포털에 로그인하고 인터넷과 기본 포털 페이지에 액세스할 수 있습니다.

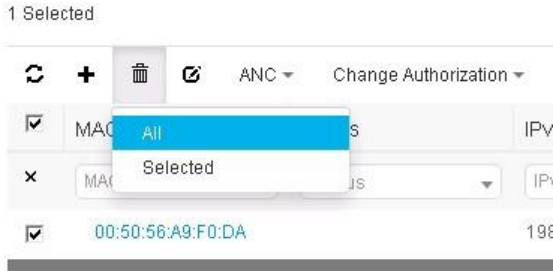
스텝

장치 정리

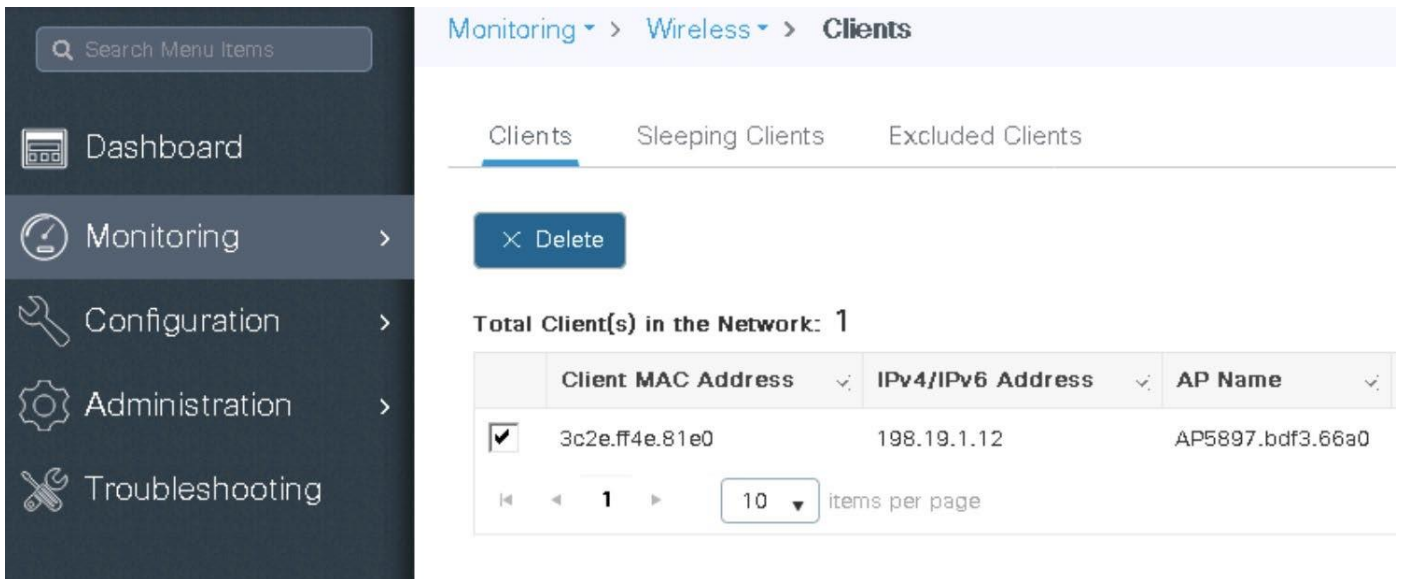
노트: 아래 지침을 주의해서 반드시 따라야합니다. 왜냐하면, 우리가 이미 다른 플로우를 거쳤으며, ISE 는 이미 장치를 프로파일링하고, 인증하고, 승인하고 엔드포인트 그룹에 추가했습니다. 다음 시나리오로 성공하려면 ISE 및 WLC 에서 장치를 완전히 제거하고 로컬 장치 설정을 삭제하는 것이 중요합니다.

1. 데모에 사용된 각 개인 사용자 **BYOD 디바이스**에 대한 **설정을 지웁니다**. 디바이스 설정이 지워지지 않으면 필요할 때 게스트 포털 또는 다른 페이지로 리디렉션되지 않을 수 있습니다.
 - a. **Web Cache** 지웁니다. [\[가이드\]](#)
 - b. 개인 디바이스 설정(**Device Settings**)을 지웁니다.. [\[가이드\]](#)
2. **Workstation1** 에서 Firefox 를 열고, 방법 중 하나를 사용하고 **admin/C1sco12345** 의 유저 ID/ 패스워드 조합을 사용하여 <https://ise.securitydemo.net> 에서 ISE 에 로그인합니다.
 - 주소 표시줄에 URL 을 수동으로 입력
 - 토폴로지 툴바에서 ISE 아이콘을 클릭
 - 북마크 툴바에서 ISE 북마크에 액세스
3. 컨텍스트 가시성(Context Visibility)> 엔드포인트(Endpoints)으로 이동합니다.
4. 모든 엔드포인트를 체크오프하고 삭제합니다.

그림: ISE 에서 엔드포인트 삭제



5. Workstation1 에서 <http://wlc1.dcloud.cisco.com> 의 WLC 로그인 페이지에 액세스합니다. 이 작업은 몇 가지 다른 방법으로 수행할 수 있습니다:
 - 주소 표시줄에 URL 을 수동으로 입력합니다.
 - 북마크 톨바에 WLC1 에 대한 북마크를 클릭합니다.
 - Firefox 에서 홈 버튼을 클릭하여 토폴로지 다이어그램으로 다시 이동한 후 vWLC 를 클릭합니다.
8. **MONITOR** 를 클릭합니다.
9. **Clients** 를 클릭합니다.
10. 클라이언트 옆의 확인란을 선택한 다음 **Delete** 를 클릭합니다.
11. **Yes** 를 클릭합니다.



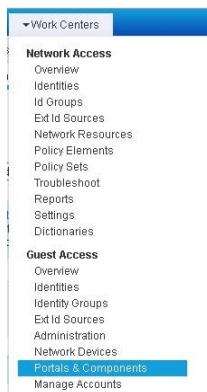
게스트 계정에 대한 자체 등록

노트: 기본적으로 스폰서는 모든 자체 등록 게스트 계정을 승인해야 합니다. 스폰서 승인(Sponsor Approval) 기능을 비활성화하려면 Disable Sponsor Approval 에 나열된 단계를 수행합니다. Sponsor Approval(스폰서 승인)이 활성화된 상태로 계속 진행하려면 게스트 등록 요청 승인(Approving the Guest Registration Request)에 나열된 단계로 건너뛴니다.

스폰서 승인 비활성화(Disable Sponsor Approval)

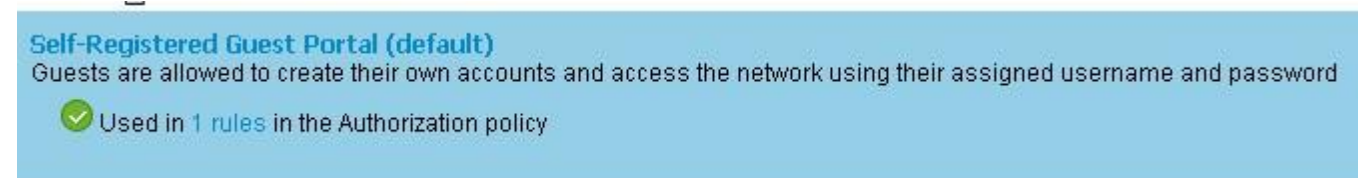
1. **Workstation1** 에서 Firefox 를 열고, 다음 방법 중 하나를 사용하고 **admin/C1sco12345** 의 유저 ID/ 비밀번호 조합을 사용하여 <https://ise.securitydemo.net> 에서 **ISE** 에 로그인합니다.
 - 주소 표시줄에 URL 을 수동으로 입력
 - 토폴로지 툴바에서 ISE 아이콘을 클릭
 - 북마크 툴바에서 ISE 북마크에 액세스
2. Work Centers>Guest Access>Portals & Components 를 클릭합니다.

그림: 포털 및 구성 요소(Portals & Components)



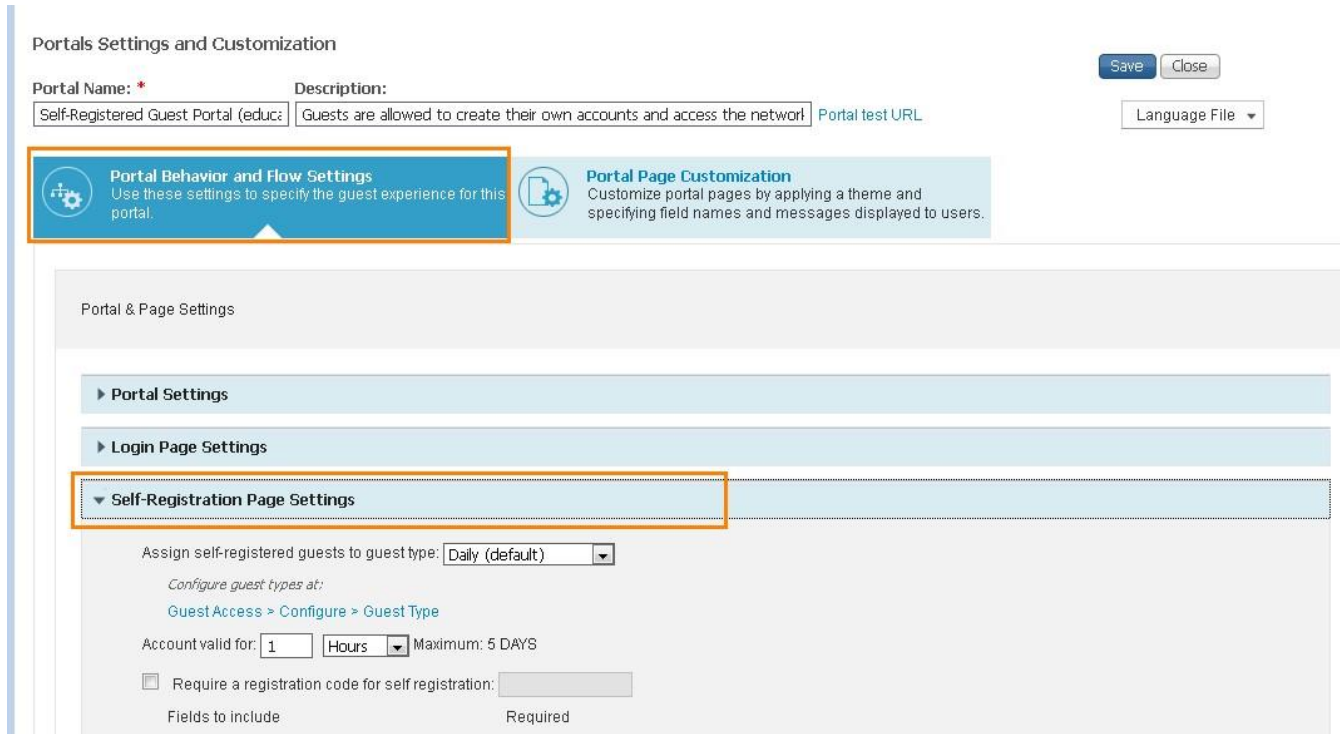
3. 목록을 스크롤하여 시나리오에 대한 '**Self-Registered Guest Portal (default)**'을 선택합니다.
4. 편집을 위해 포털을 클릭합니다.

그림: 게스트 포털



5. Portal Behavior(포털 동작) 및 Flow Settings(플로우 설정)에서 아래로 스크롤하여 Self-Registration Page Settings(자체 등록 페이지 설정)으로 이동합니다.

그림: Portal Behavior 및 Flow Settings



6. Require self-registered guests to be approved(자체 등록 게스트 승인 필요) 확인란 선택을 취소합니다.

그림: 게스트 등록 비활성화 (Disable Guest Registration)



AP 및 실제 클라이언트 엔드포인트 장치 없이 게스트 시연

노트: 연결된 게스트 포털에서 포털 테스트 URL 을 사용하여 AP 또는 클라이언트 엔드포인트 없이 게스트 플로우를 통과할 수 있습니다.

노트: 최상의 사용자 경험과 데모를 위해 실제 클라이언트와 함께 AP 를 사용하는 것이 좋습니다.

노트: RADIUS Live Logs 및 Guest 보고서에는 RADIUS 세션이 없기 때문에 정보가 제한됩니다.

노트: 리얼 클라이언트를 리디렉션하기 위해 무선 세션이 필요하며 전체 액세스 권한이 있는 시스템에서 포털을 사용하는 경우 네트워크 리소스에 대한 제한된 액세스를 시연할 수 없기 때문에 성공 플로우가 정적 또는 원본 URL 로 보낼 수 없습니다. 시뮬레이션된 플로우이므로 액세스 제어가 적용되지 않습니다.

8. 모니터링 시스템 브라우저 또는 dCloud Workstation 을 사용하여 ISE portal 로 이동합니다.

9. Work Centers > Guest Access > Portals & Components 로 이동합니다.

- 수직 맞춤 요구 사항에 따라 원하는 **Self-reg portal** 를 클릭합니다.
- Portal test URL link** 를 클릭합니다. 이는 다른 창에서 포털이 열립니다.



- 이제, 다음 단계를 통해 실제 디바이스에 적용되는 정보를 건너뛰면서 빠른 Self-reg 플로우를 수행할 수 있습니다. 일부 정보는 적용되지 않고 보고 정보도 제한된 것을 유의해야 합니다.

SSID dCloud-Guest 에 연결

- 유저 장치를 개방형 무선 SSID **dCloud-Guest** 에 연결합니다.

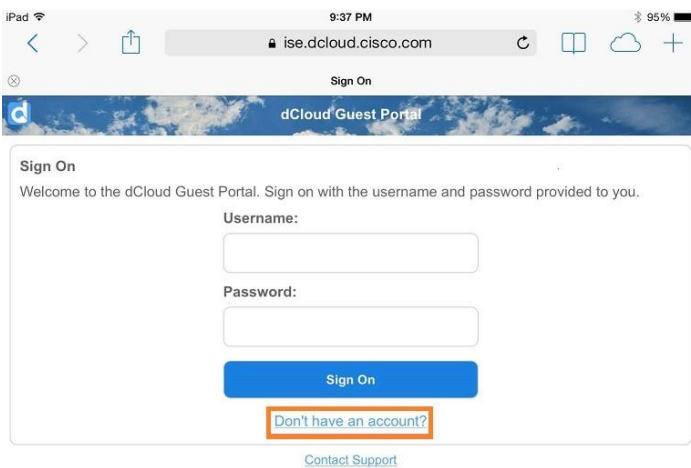
노트: 데모 전체에서 특정 DCloud WiFi 신호에 연결됩니다. 우리는 일반적으로 언급하지만 **DCloud-Guest-123456** 과 같은 고유한 세션 ID 가 부가됩니다.

- 사용자 장치에 지원되는 내장된 웹 브라우저를 열고 아무 웹 페이지를 탐색합니다. 그러면 **dCloud Guest Portal** 로 리디렉션됩니다.

노트: 브라우저를 열 때 HTTP 를 사용하여 페이지에 액세스해야 합니다. **HTTPS** 를 사용하여 페이지에 액세스하면 핫스팟 포털로 리디렉션되지 않습니다. 이는 **HTTPS** 리디렉션을 처리하는 WLC 에서 알려진 문제입니다.

- 로그인 버튼 아래에 있는 **Don't have an account?** 를 클릭합니다.

그림: 게스트 포털(Guest Portal) 로그인 페이지



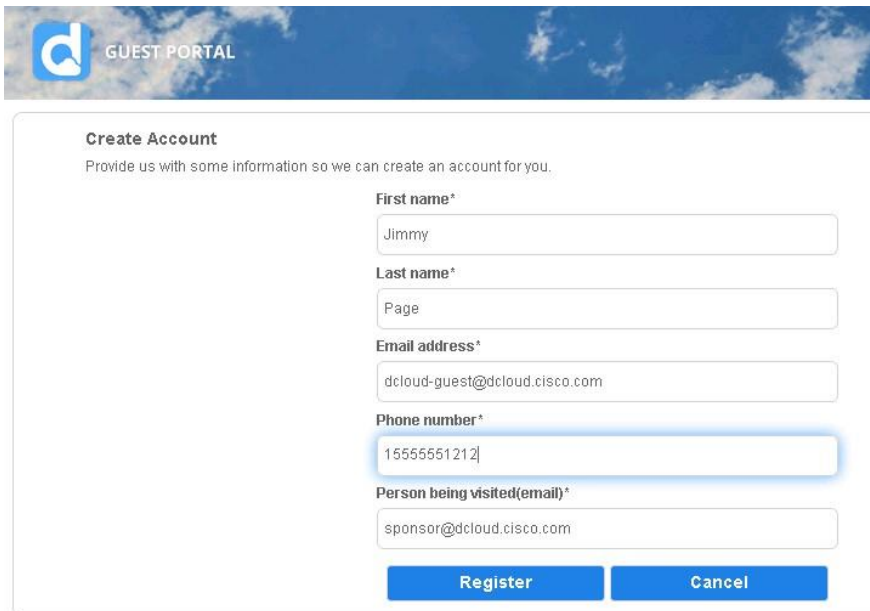
- 다음과 같은 조건으로 게스트 계정에 필요한 정보를 입력합니다:

- 이메일 주소는 공개적으로 액세스할 수 있는 모든 이메일 계정 또는 이 데모에 사전에 구성된 내장 dcloudguest@dcloud.cisco.com 계정일 수 있습니다.
- 전화 번호는 SMS 를 통해 게스트 자격 증명을 받을 수 있는 고객이 원하는 실제 전화 번호여야 합니다. 공백이나 대시 없이 국가 코드 + 지역 번호 + 전화 번호를 입력하십시오(예: 15865551234).
- 스폰서 승인 (Sponsor Approval)으로 자체 등록을 수행하는 경우 sponsor@dcloud.cisco.com 을 입력해야 합니다.

노트: 아래의 스크린샷 및 단계는 사용자가 내장된 dcloud-guest@dcloud.cisco.com 계정 및 이메일 주소를 사용하여 게스트 자격 증명을 받는 것을 보여줍니다. 다른 공용 이메일 주소를 사용하는 경우 게스트 자격 증명을 받으려면 해당 이메일 계정에 로그인해야 합니다. 두 경우 모두 데모 초기에 해당 기능을 비활성화하지 않은 한 스폰서 계정을 사용하여 데모에서 OWA 에 로그인하여 게스트 등록을 승인해야 합니다. 외부 제공업체에게 게스트 알림을 보내는 경우 전달된다는 보장은 없습니다. 시도하기 전에 이를 테스트하는 것을 권장하며, 실패하는 경우, 내장된 서버를 사용하십시오.

5. **Register** 를 클릭합니다.

그림: Guest Self-Registration 페이지



노트: 게스트 자격 증명은 게스트 사용자에게 이메일 및 SMS 메시지로 전송됩니다. 공용 이메일 주소를 사용하지 않으려는 경우 게스트 자격 증명을 사용하여 이메일을 수신하기 위한 데모 환경 내에 게스트 계정이 설정되어 있습니다. 자격 증명 전송되면 Microsoft Exchange OWA 를 통해 게스트 이메일 계정에 로그인하여 자격 증명에 포함된 이메일을 확인할 수 있습니다. 전화 번호를 올바른 형식으로 입력하지 않으면 SMS 를 받을 수 없습니다.

6. 게스트 등록 요청을 제출하면 **sign-in 페이지**에 로그인 자격 증명에 포함된 이메일 또는 SMS 메시지가 전송되었다는 **메모가 표시**됩니다.

노트: 1-7 단계에서 스폰서 승인(Sponsor Approval)을 비활성화하지 않은 경우, 스폰서가 다음 단계에서 게스트 등록 요청을 승인할 때까지 SMS 또는 이메일을 받지 못합니다. 스폰서 승인을 비활성화한 경우 다음 섹션에서 7 단계로 건너뛸 수 있습니다.

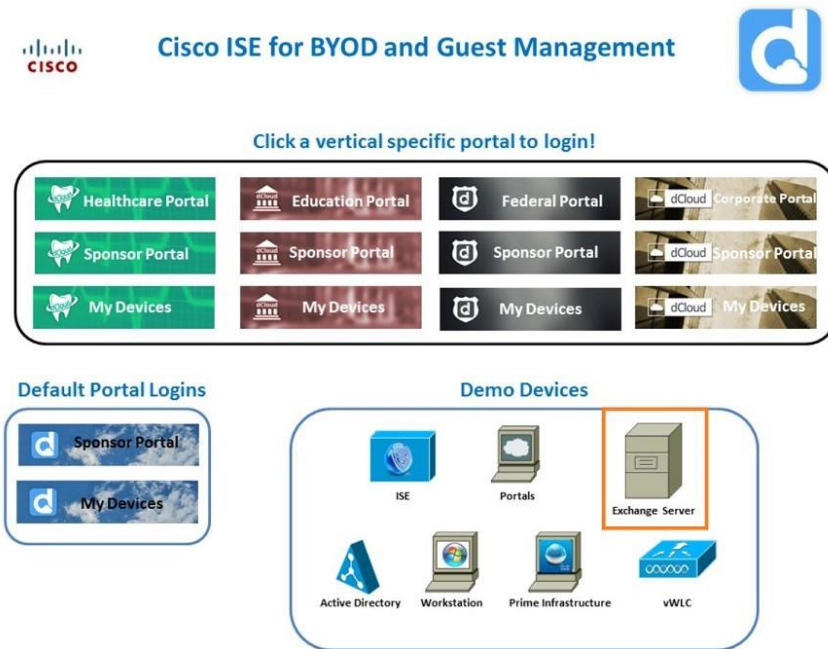
게스트 등록 요청 승인

13. **Workstation1** 에서 Firefox 를 열고 홈 버튼을 클릭하여 홈페이지로 이동합니다.

14. **Demo Devices** 에서 **Exchange Server** 를 클릭하여 별도의 페이지에서 Outlook Web App 을 엽니다.

노트: Outlook Web App 로그인 페이지를 표시하는 데 약 10 초가 걸릴 수 있습니다.

그림: Exchange Server 아이콘을 클릭



15. Outlook Web App 에 로그인 합니다(**dcloudWsponsor / C1sco12345**).

그림: Exchange OWA 웹 로그인 페이지



16. 이메일 Inbox 에서 **Guest Approval Request** 이메일을 엽니다. 승인을 위해 이메일 메시지 하단에 있는 링크를 클릭하여 계정을 활성화합니다.

그림: 스폰서 메일박스 내 Guest approval 이메일

Please approve (or deny) this self-registering guest. The guest provided the following information:

Username: jpage
First Name: Jimmy
Last Name: Page

[Approve](#)

[Deny](#)

Otherwise, Please go to <https://sponsor.dcloud.cisco.com> to approve or deny this request.
Thank You for using Cisco dCloud!

그림: 승인된 게스트 계정



Guest (jpage) has been approved.

[Help](#)

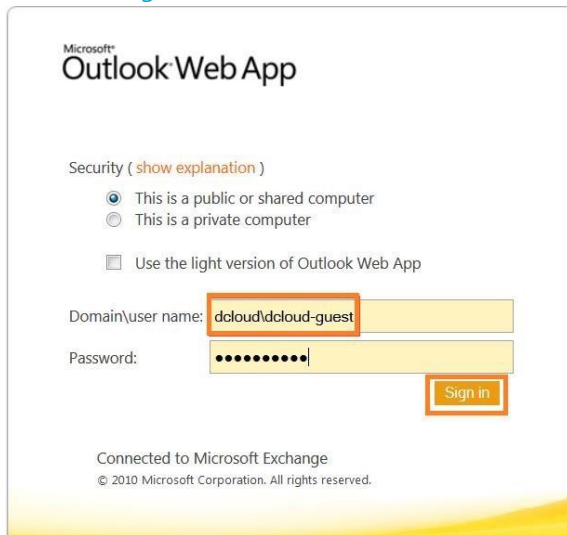
17. 게스트 사용자 자격 증명이 포함된 SMS 텍스트 메시지를 수신해야 합니다. **SMS 를 받는 데 최대 1 분이 걸릴 수 있습니다.**

노트: 이 데모 환경을 제어할 수 없는 여러 가지 이유로 인해 모바일 디바이스가 SMS 를 수신하지 못할 수 있습니다. 디바이스 번호를 올바르게 입력한 경우 휴대폰 공급자 또는 계정 관련 개인 설정으로 인해 메시지를 수신하지 못할 수 있습니다. 예를 들어, 등록된 휴대전화는 '통화 안 함('do not call')' 목록에 있는 경우입니다.

18. 또한 등록된 이메일 주소로 이메일이 전송됩니다. 전자 메일에 액세스하려면 다음을 수행합니다:
- Workstation1 로 돌아가서 오른쪽 상단의 Sign Out 을 클릭하여 스폰서 계정에 로그아웃 합니다.
 - Outlook WebMail 의 북마크를 클릭하여 로그인 페이지로 돌아갑니다.
 - dcloud\ddcloud-guest 및 C1sco12345 자격 증명을 사용하여 로그인합니다.
 - 만약 게스트 사용자를 공용 이메일 주소로 등록한 경우 공용 이메일 주소의 받은 편지함으로 이동하여 ISE 에서 받은 게스트 자격 증명에 포함된 이메일을 찾습니다.

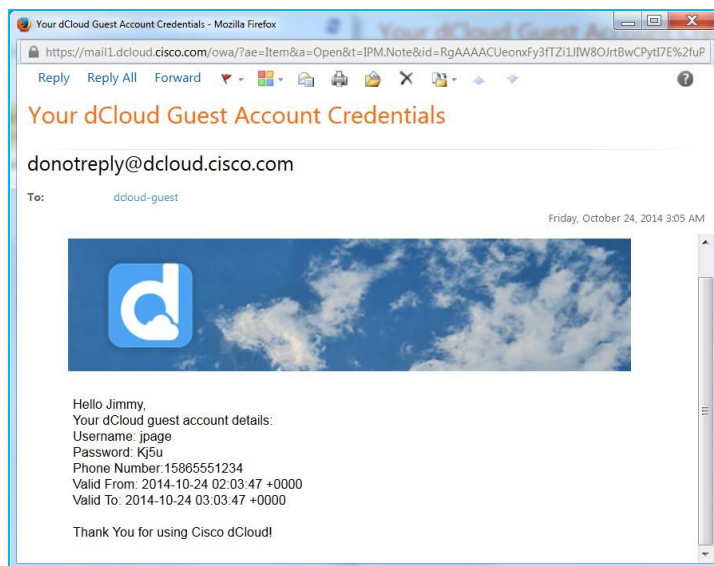
노트: 다음 단계에서는 공용 이메일 주소를 사용하지 않았다고 가정하며 OWA 를 통해 dcloud-guest 계정에 로그인하는 방법을 보여 줍니다.

그림: Exchange OWA 웹 로그인 페이지



19. Inbox 에서 게스트 자격 증명에 포함된 이메일을 찾아야 합니다.

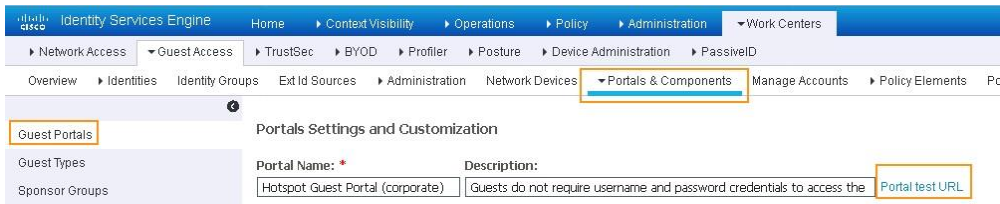
그림: 자격 증명을 포함한 게스트 계정 이메일 승인



AP 및 리얼 클라이언트 엔드포인트 장치없이 게스트 시연

노트: 연결된 게스트 포털의 포털 테스트 URL 을 사용하여 AP 또는 클라이언트 엔드 포인트없이 게스트 플로우를 통과할 수 있습니다. 그러나, 최상의 사용자 경험과 데모를 위해 리얼 클라이언트와 함께 AP 를 사용하는 것이 좋습니다. RADIUS Live Logs 및 게스트 보고서에는 RADIUS 세션이 없으므로 정보가 제한됩니다. 또한 실제 클라이언트를 리디렉션하는 데 필요한 무선 세션이 있기 때문에 성공 플로우는 정적 또는 원본 URL 로 보낼 수 없습니다. 또한 전체 액세스 권한이 있는 시스템에서 포털을 사용하므로 네트워크 리소스에 대한 제한된 액세스를 시연할 수도 없습니다. 시뮬레이션된 플로우이므로 액세스 제어가 적용되지 않습니다.

20. 모니터링 시스템 브라우저 또는 dCloud Workstation 을 사용하여 **ISE portal** 로 이동합니다.
21. Work Centers > Guest Access > Portals & Components 으로 이동합니다.
22. 원하는 **Self-reg portal** 를 클릭합니다. (수직 맞춤 요구 사항에 따라).
23. **Portal test URL link** 를 클릭합니다. -이는 포털을 다른 창에서 열리도록 합니다..

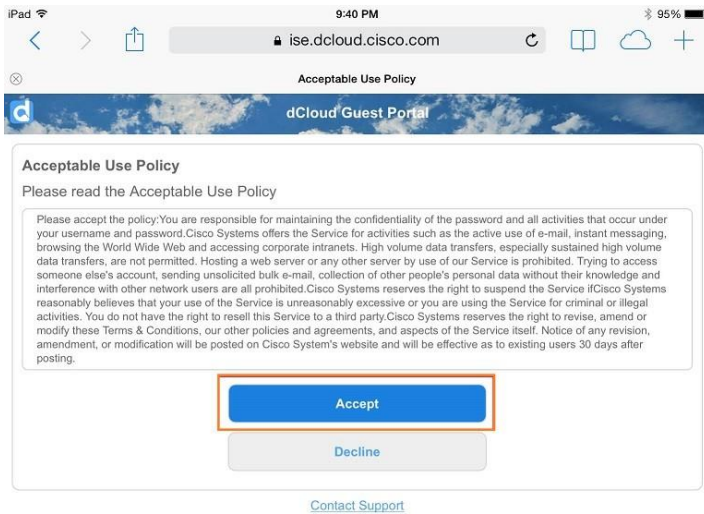


24. 이제 다음 단계를 통해 실제 장치에 적용되는 정보를 건너뛰면서 빠른 Self-reg 플로우를 수행할 수 있습니다. 일부 정보는 적용되지 않고 보고 정보도 제한됩니다.

게스트 네트워크 액세스

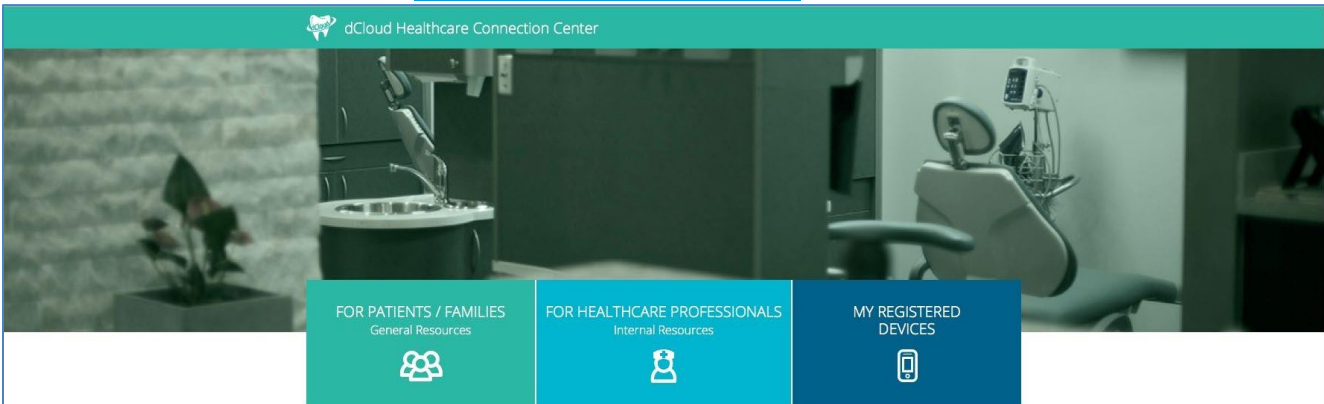
25. 사용자 디바이스에서 SMS/Email 을 통해 받은 자격 증명을 사용하여 게스트 포털에 로그인합니다.
26. **Acceptable use policy** 를 승인을 위해 **Accept** 를 클릭한 다음 **Continue** 를 클릭합니다. **Success** 페이지는 네트워크를 통해 인터넷에 액세스할 수 있음을 나타냅니다..

그림: Guest Portal acceptable use policy



27. www.cisco.com 에 대한 링크를 클릭하여 장치가 게스트 포털을 통해 인터넷에 액세스할 수 있음을 보여줍니다.
28. **Main Portal URL**(사용 가능한 포트 테이블 참조)과 선택한 시나리오(헤스케, 교육, 연방 또는 기업)으로 이동합니다. 보안 경고가 발생하면 **Continue** 를 클릭합니다.
29. **General Resources** 를 선택하여 이제 사용자에게 일반 리소스(general resources) 페이지에 대한 액세스 권한이 있음을 보여줍니다.
30. **Internal Resources** 또는 **My Registered Devices** 를 선택하여 사용자가 이 페이지에 액세스할 수 없음을 보여줍니다.

그림: Healthcare Connections Center: <http://health.dcloud.cisco.com>



ISE의 자체 등록 게스트 플로우 시연

이제 디바이스가 게스트 네트워크에 성공적으로 접속되어 인터넷에 액세스할 수 있습니다. 다음으로, ISE UI에 대해 간략하게 살펴보고, ISE가 디바이스를 동적으로 프로파일링하고 적절한 인증 프로파일을 적용하여 게스트 인터넷 액세스를 동적으로 허용한 기본 사항을 설명하겠습니다.

31. **Workstation1**에서 Firefox를 열고 User ID/ 패스워드를 **admin/ C1sco1234**로 조합하여 사용하고 다음 방법 중 하나를 사용하여 <https://ise.securitydemo.net>에서 ISE에 로그인 합니다:

- 주소 표시줄에 URL 을 수동으로 입력
- 토폴로지 툴바에서 ISE 아이콘을 클릭
- 북마크 툴바에서 ISE 북마크에 액세스

32. 마우스를 **Operations** 메뉴 위에 올려 **RADIUS Livelog** 를 클릭합니다. 이 화면은 ISE 의 최근 인증 및 인증 시도를 표시됩니다.

노트: 이 특별한 데모 경우에는 Apple iPad 를 사용하여 게스트 네트워크에 연결합니다.

장치가 처음 dCloud-Guest SSID 에 가입하면 MAB(MAC authentication bypass)를 사용하여 인증하고 ISE 는 **GUEST_REDIRECT** 프로파일을 WLC 에 반환합니다. 이는 WLC 가 모든 사용자 웹 트래픽을 **dCloud Guest Portal** 로 리디렉션하도록 지시합니다.

잠시 후, ISE 는 디바이스를 Apple iPad 라고 올바르게 프로파일링합니다. 이 데모에서는 장치 유형 기능에 따라 차별화된 액세스를 보여주지 않습니다.

사용자가 자체 등록 후, 스폰서의 승인을 받고 GUEST_ACCESS 라는 게스트 포털에 로그인합니다. 이 프로파일은 인터넷 및 기본 포털에만 액세스할 수 있도록 WLC 에 미리 구성된 ACL 이름을 푸시합니다. 아래의 스크린샷에서는 스폰서로부터 게스트 액세스 승인을 받은 후 "jpage1" 사용자가 로그인한 것을 확인할 수 있습니다.

그림: Dynamic Application of Guest Access

Time	Status	Details	Identity	Endpoint ID	Authentication Policy	Endpoint Profile	Authorization Policy	Authorization Profiles
Mar 26, 2018 07:15:42:151 AM			jpage1	DC:A4:CA:D2:5F:9D	Guest Access	Apple-iPad	Guest Access >> Guest Access	GUEST_ACCESS
Mar 26, 2018 07:15:42:142 AM			jpage1	DC:A4:CA:D2:5F:9D	Guest Access	Apple-iPad	Guest Access >> Guest Access	GUEST_ACCESS
Mar 26, 2018 07:15:42:133 AM			jpage1	DC:A4:CA:D2:5F:9D	Guest Access	Apple-iPad	Guest Access >> Guest Access	GUEST_ACCESS
Mar 26, 2018 07:15:37:414 AM			jpage1	DC:A4:CA:D2:5F:9D	Guest Access	Apple-iPad	Guest Access >> Guest Redirect	GUEST_REDIRECT
Mar 26, 2018 07:13:04:689 AM			DC:A4:CA:D2:5F:9D	DC:A4:CA:D2:5F:9D	Guest Access >> MAB	Apple-iPad	Guest Access >> Guest Redirect	GUEST_REDIRECT

시나리오 3. 스폰서 게스트 액세스

가치 제안: 이 시나리오에서 조직은 필요에 따라 게스트 사용자 계정을 프로비저닝할 필요가 있습니다. 게스트 사용자 계정은 도착하기 전에 사무실 방문자를 위해 설정될 수 있으며 기본적인 인터넷 액세스를 제공합니다. 특히 이 시나리오에서 조직은 자체 등록이 아닌 그들이 도착하기 전에 게스트 계정을 제공함으로써 종업원이 게스트 사용자를 지원하도록 하는 것을 선호한다.

게스트 계정은 스폰서가 계획된 도착 시간 전에 생성하며 게스트 사용자는 SMS 와 이메일을 통해 로그인 자격 증명을 전송합니다. 게스트 사용자는 도착하면 dCloud-Guest SSID 에 연결하고 로그인한 다음 네트워크에 액세스할 수 있습니다. 또한, ISE 스폰서 포털에서 사용자 계정을 대량 가져올 수 있습니다. 이 기능은 여러 게스트 사용자 계정을 동시에 프로비저닝하는 데 유용합니다. 예를 들어, 사무실 관리자가 대규모 영업 이벤트 전날에 50 개의 새로운 게스트 계정을 프로비저닝해야 하는 원격 영업 사무소에 유용할 수 있습니다.

노트: 게스트 액세스는 각 개별 조직에서 정의하는 다양한 유형의 인증된 액세스를 의미합니다. 이 데모에서는 게스트 액세스가 게스트에게 인터넷 및 메인 포털 페이지를 방문할 수 있는 기능을 제공합니다. 일부 조직에서는 게스트 액세스를 인터넷으로만 정의하는 반면, 다른 조직에서는 인터넷뿐만 아니라 특정 내부 리소스에 대한 액세스 권한도 부여할 수 있습니다. ISE 는 유연하며 고객 요구 사항에 따라 구성할 수 있습니다.

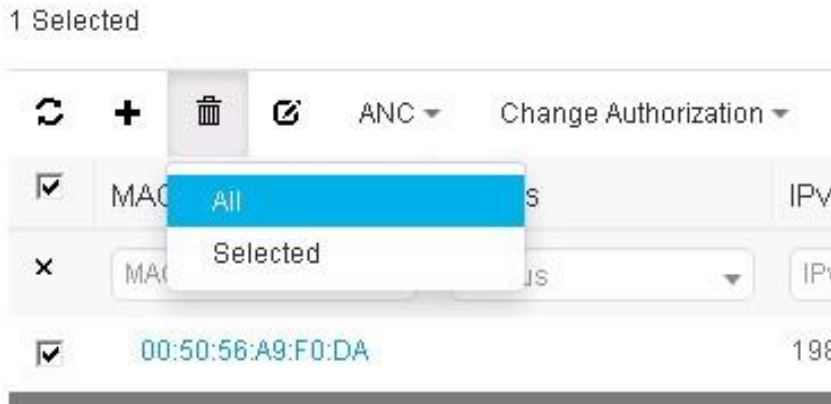
스텝

디바이스 정리

노트: 아래 지침을 주의해서 반드시 따라야합니다. 왜냐하면, 우리가 이미 다른 플로우를 거쳤으며, ISE 는 이미 장치를 프로파일링하고, 인증하고, 승인하고 엔드포인트 그룹에 추가했습니다. 다음 시나리오로 성공하려면 ISE 및 WLC 에서 장치를 완전히 제거하고 로컬 장치 설정을 삭제하는 것이 중요합니다. 이 단계를 제대로 따르지 않으면 데모가 설계된대로 작동하지 않을 수 있습니다.

33. 데모에 사용된 각 개인 사용자 **personal device** 에 대한 **settings** 를 지웁니다. 디바이스 설정이 지워지지 않으면 필요할 때 게스트 포털 또는 다른 페이지로 리디렉션되지 않을 수 있습니다.
 - a. **Web Cache** 를 지웁니다. [\[가이드\]](#)
 - b. 개인 디바이스 설정(**Personal Device Settings**)을 지웁니다. [\[가이드\]](#)
34. **Workstation1** 에서 Firefox 를 열고, 아래의 방법 중 하나를 사용하여 **admin/C1sco12345** 의 유저 ID/패스워드 조합으로 <https://ise.securitydemo.net> 에서 ISE 에 로그인합니다.
 - 주소 표시줄에 URL 을 수동으로 입력
 - 토폴로지 툴바에서 ISE 아이콘을 클릭
 - 북마크 툴바에서 ISE 북마크에 액세스
35. 컨텍스트 가시성(Context Visibility)> 엔드포인트(Endpoints)으로 이동합니다.
36. 모든 엔드포인트를 체크오프하고 삭제합니다.

그림: ISE 에서 엔드 포인트 삭제



37. Workstation1 에서 <http://wlc1.dcloud.cisco.com> 으로 이동하여 WLC 로그인 페이지를 액세스합니다. 이 작업은 다른 같은 몇 가지 방법으로 수행할 수 있습니다:
 - a. 주소 표시줄에 URL 을 수동으로 입력합니다.
 - b. 북마크 톨바에 WLC-9800-CL 에 대한 북마크를 클릭합니다.
 - c. Firefox 에서 홈 버튼을 클릭하여 토폴로지 다이어그램으로 돌아가서 vWLC 를 클릭합니다.
38. 데모 준비 중 엔드포인트를 프로비저닝하는 데 사용된 것과 동일한 **디바이스별 자격 증명**을 사용하여 vWLC 에 로그인합니다.
39. 상단 메뉴바에서 Monitoring > Wireless > Client 를 클릭합니다.
40. 이전에 데모 네트워크에 가입한 모든 클라이언트가 나열됩니다. 연결된 클라이언트에 대한 확인란을 선택한 다음 **Delete** 를 클릭합니다.

그림: C9800-CL 에서 클라이언트 삭제

Guest Accounts 만들기

41. **Workstation1** 에서 Firefox 를 열고 **Home** 버튼을 클릭합니다.
42. 기본 포털 로그인 섹션(Default Portal Logins)에서 스폰서 포털(Sponsor Portal)을 클릭합니다.

그림: 토폴로지 페이지

43. 사용자 ID/패스워드를 **sponsor/ C1sco12345** 의 조합을 사용하여 **Sponsor Portal** 에 로그인합니다.

노트: 계정 관리(Manage Accounts)에서 Guest Type 을 변경할 수 없습니다. (본 데모에서는 이 기능을 사용할 수 없음)

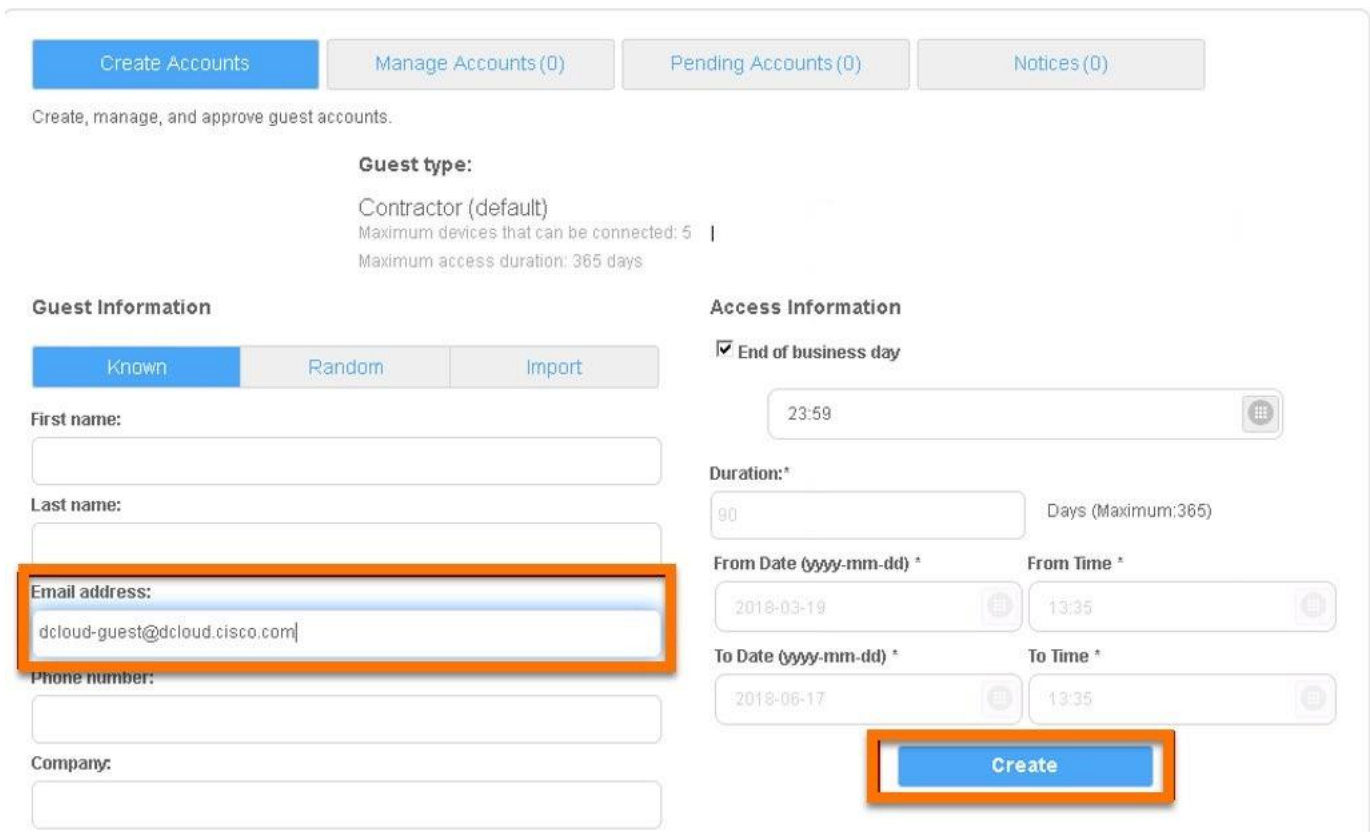
44. **Create Accounts** 탭에서 다음과 같은 조건으로 게스트 계정에 필요한 정보를 입력합니다:

- 이메일 주소는 공개적으로 액세스할 수 있는 모든 이메일 계정 또는 이 데모에 미리 구성된 기본 제공 계정 dcloudguest@dcloud.cisco.com 일 수 있습니다.
- 전화 번호는 SMS 를 통해 게스트 자격 증명을 받을 수 있는 고객이 원하는 실제 전화 번호여야 합니다. 국가 코드 + 지역 코드 + 공백이나 대시 없이 전화 번호를 입력해야 합니다. (예: 15865551234).

45. 정보 입력이 완료되면 **Create** 를 클릭하여 게스트 계정을 생성하고 **Account Information**(계정 정보) 화면을 엽니다.

노트: 영어를 기본 언어로 남겨 두는 것을 권장합니다. 영어 이외의 언어를 선택하면 SMS 메시지에 예기치 않은 문자가 포함될 수 있습니다.

그림: 스폰서 포털에서 게스트 계정 생성하기



46. **Notify** 를 클릭합니다.

그림: 게스트에게 계정 생성 성공 알림

Account Information

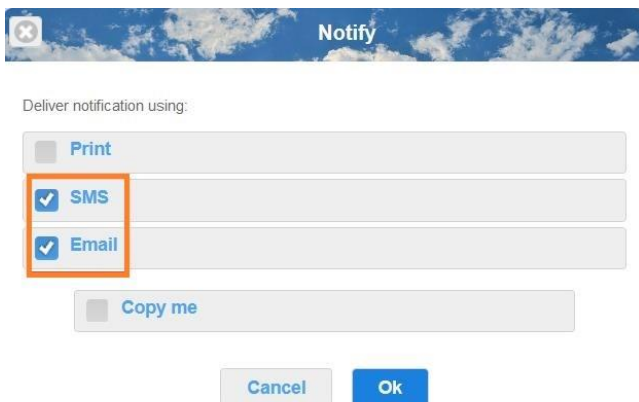
Username:	rp1ant
Password:	x8aJ
First name:	Robert
Last name:	Plant
Email address:	dcloud-guest@dcloud.cisco.com
Company:	
Phone number:	15865551234
Guest type:	Contractor (default)
SMS provider:	Global Default
State:	Created
From date (yyyy-mm-dd):	2014-10-23 22:31
To date (yyyy-mm-dd):	2015-01-20 20:35
Location:	London
SSID:	
Language:	English
Group tag:	
Time left:	88D 17H 59M

47. **Notify** 박스에서 **SMS** 및 **Email** 를 확인합니다.

48. 게스트 사용자 자격 증명에 포함된 SMS 문자 메시지 및 이메일을 보내려면 **OK** 를 클릭하십시오. SMS 를 받는 데 최대 1 분이 걸릴 수 있습니다.

노트: 모바일 장치가 이 데모 환경을 제어할 수 없는 여러 가지 이유로 인해 SMS 를 수신하지 못할 수 있습니다. 장치 번호를 올바르게 입력한 경우 휴대폰 공급자 또는 계정 관련 개인 설정으로 인해 메시지를 수신하지 못할 수 있습니다. 예를 들어 등록된 휴대전화는 '통화 안 함' 목록에 있는 경우 수신하지 못할 수 있습니다.

그림: Notify 팝업 창



노트: 자격 증명에 전송되면 게스트 이메일 계정에 로그인하여 자격 증명에 포함된 이메일을 검색할 수 있습니다. 전화 번호를 올바른 포맷으로 입력하지 않으면 SMS 가 수신되지 않습니다. 다음 단계에서는 게스트 계정 등록에 내장된 dcloud-guest@dcloud.cisco.com 계정을 사용했다고 가정합니다. 공용 이메일 주소를 사용한 경우, 해당 전자 메일 계정의 inbox 로 이동하여 게스트 자격 증명에 포함된 이메일을 찾아야 합니다.

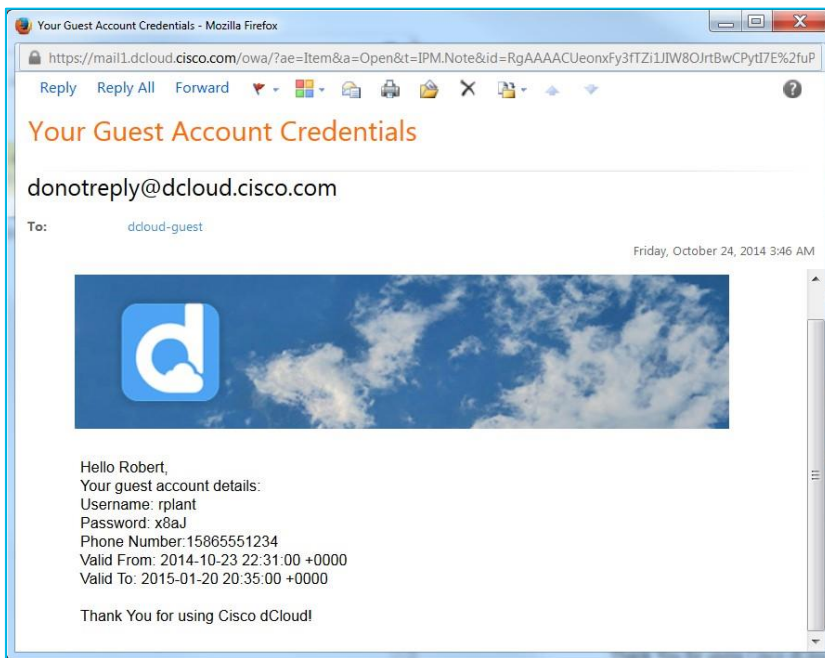
49. Outlook Web Mail 의 북마크를 클릭하고 **dcloud@dcloud-guest** 및 **C1sco12345** 의 사용자 ID/패스워드 조합을 사용하여 로그인 후 이메일에 액세스합니다.

그림: Exchange OWA Web 로그인 페이지



50. 게스트 자격 증명이 포함된 이메일을 엽니다.

그림: 자격 증명 포함된 게스트 이메일 승인

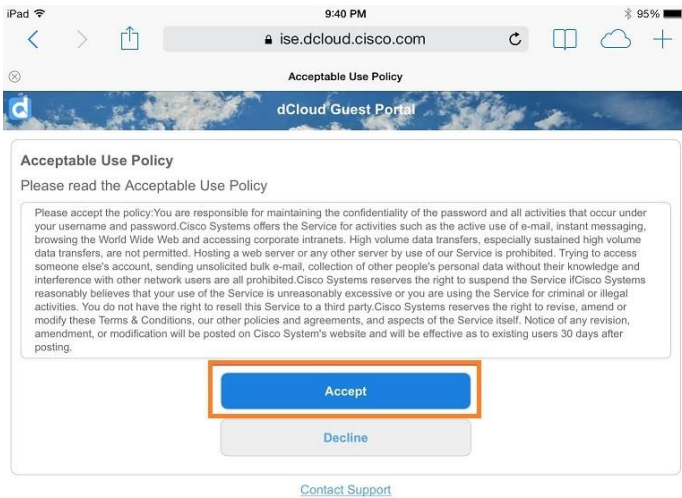


51. 사용자 디바이스에서 **SSID dCloud-Guest** 에 연결합니다. 게스트 포털로 리디렉션할 Safari 를 열고 알림에 수신된 자격 증명으로 게스트 포털에 로그인합니다.

노트: 시연 내내 특정 DCloud WiFi 시그널에 연결됩니다. 일반적으로는 **dCloud-Hotspot-123456** 과 같은 고유한 세션 ID 가 추가됩니다.

52. **Accept** 를 클릭하여 **acceptable use policy** 을 승인한 다음 **Continue** 를 클릭합니다. **Success** 페이지는 네트워크를 통해 인터넷에 액세스할 수 있음을 나타냅니다.

그림: Guest Portal acceptable use policy



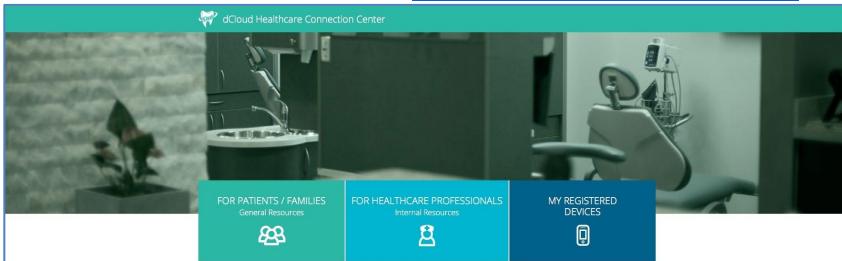
53. www.cisco.com 에 대한 링크를 클릭하여 디바이스가 이제 게스트 포털을 통해 인터넷에 액세스할 수 있음을 보여줍니다.

54. **Main Portal URL** (사용 가능한 포털 표에 표시됨)과 선택한 시나리오(헤스케어, 교육, 연방 또는 기업)으로 이동합니다. 보안 경고가 발생하면 **Continue** 를 클릭합니다.

55. **General Resources** 를 선택하여 이제 사용자에게 이 페이지에 대한 액세스 권한이 있음을 표시합니다.

56. **Internal Resources** 또는 **My Registered Devices** 를 선택하여 사용자가 이러한 페이지에 액세스할 수 없음을 표시합니다.

그림: Healthcare Connections Center: <http://health.dcloud.cisco.com>



ISE 에서 스폰서 게스트 플로우 시연

디바이스가 게스트 네트워크에 성공적으로 연결되어 인터넷에 액세스할 수 있습니다. 이 섹션에서는, ISE 가 적절한 인증 프로파일을 적용하여 장치를 동적으로 프로파일링하고 게스트 인터넷 액세스를 동적으로 허용하는 방법의 기본 사항을 보여주기 위해 ISE UI 에 대해 간략하게 살펴보겠습니다.

57. **Workstation1** 의 데스크톱에서 Firefox 를 시작합니다.

58. **Workstation1** 에서 Firefox 를 열고, **admin/C1sco12345** 를 사용자 ID/ 패스워드 조합으로 사용하고 다음 방법 중 하나를 사용하여 <https://ise.securitydemo.net> 에서 ISE 에 로그인합니다:

- 주소 표시줄에 URL 을 수동으로 입력
- 토폴로지 툴바에서 ISE 아이콘을 클릭
- 북마크 툴바에서 ISE 북마크에 액세스

59. **Operations** 메뉴 위로 마우스를 올려 **RADIUS Livelog** 를 클릭합니다. 이 화면에는 ISE 의 최신 인증 및 권한 부여 시도가 표시됩니다.

노트: 특히 이 경우에는 Apple iPad 를 사용하여 게스트 네트워크에 연결 했습니다. 디바이스가 처음 dCloud-Guest SSID 에 연결하면 MAB(MAC authentication bypass)를 사용하여 인증되고 ISE 가 **GUEST_REDIRECT** 프로파일을 WLC 에 반환합니다. 이는 WLC 가 **모든 사용자 웹 트래픽을 dCloud Guest Portal** 로 리디렉션하도록 지시합니다.

잠시 후, ISE 는 장치를 Apple iPad 로 올바르게 프로파일링합니다. 이 데모에서는 장치 유형 기능에 따라 차별화된 액세스는 표시하지 않습니다.

스폰서가 프로비저닝한 계정을 사용하여 게스트 포털에 로그인한 후 ISE 는 엔드 포인트를 다시 인증하고 GUEST_ACCESS 라는 프로파일을 동적으로 할당하는 COA 를 전송합니다. 이 프로파일은 인터넷 및 기본 포털에만 액세스할 수 있도록 WLC 에 미리 구성된 ACL 이름을 푸시합니다.

아래 스크린샷은 스폰서 포털에서 스폰서가 게스트 계정을 만든 후 jpage1 사용자가 로그인 한 방법을 보여줍니다.

그림: Dynamic Guest Access Application

Time	Status	Details	Identity	Endpoint ID	Authentication Policy	Endpoint Profile	Authorization Policy	Authorization Profiles
Mar 26, 2018 07:15:42.151 AM			jpage1	DC:A4:CA:D2:5F:9D	Guest Access	Apple-iPad	Guest Access >> Guest Access	GUEST_ACCESS
Mar 26, 2018 07:15:42.142 AM			jpage1	DC:A4:CA:D2:5F:9D	Guest Access	Apple-iPad	Guest Access >> Guest Access	GUEST_ACCESS
Mar 26, 2018 07:15:42.133 AM			jpage1	DC:A4:CA:D2:5F:9D	Guest Access	Apple-iPad	Guest Access >> Guest Access	GUEST_ACCESS
Mar 26, 2018 07:15:37.414 AM			jpage1	DC:A4:CA:D2:5F:9D	Guest Access >> MAB	Apple-iPad	Guest Access >> Guest Redirect	GUEST_REDIRECT
Mar 26, 2018 07:13:04.689 AM			DC:A4:CA:D2:5F:9D	DC:A4:CA:D2:5F:9D	Guest Access >> MAB	Apple-iPad	Guest Access >> Guest Redirect	GUEST_REDIRECT

대량 게스트 계정 만들기

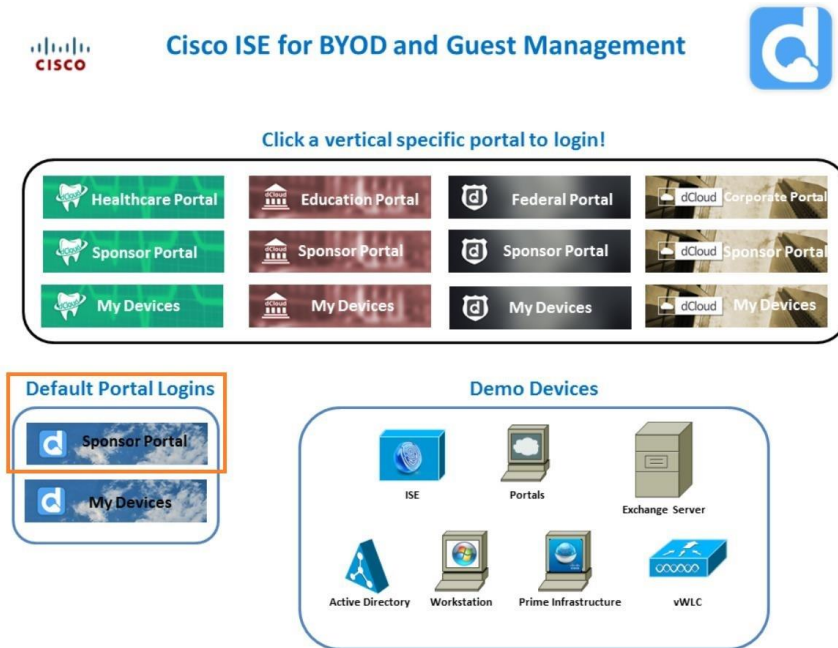
ISE 스폰서 포털은 대량 가져오기 기능을 사용하여 여러 게스트 계정을 동시에 프로비저닝할 수 있습니다. 스폰서는 ISE 스폰서 포털에서 .csv 템플릿을 다운로드할 수 있습니다. 이 포털에는 ISE 가 다양한 게스트 계정을 만드는 데 필요한 특정 정보에 대한 칼럼(columns)이 포함되어 있습니다. 스폰서는 이 템플릿을 사용하여 성함, 성, 전화 번호 등 게스트 계정에 필요한 모든 정보를 입력할 수 있습니다.

.csv 파일 완료 후 스폰서는 .csv 파일을 ISE 스폰서 포털로 가져오고 ISE 는 스프레드시트의 모든 사용자에게 대한 게스트 계정을 생성합니다. 이 데모에서는 이미 8 개의 게스트 사용자 계정이 포함된 **Workstation1** 데스크톱에 사전 구축된 .csv 파일을 사용합니다.

60. **Workstation1** 에서 Firefox 를 열고 **Home(홈)** 버튼을 클릭합니다.

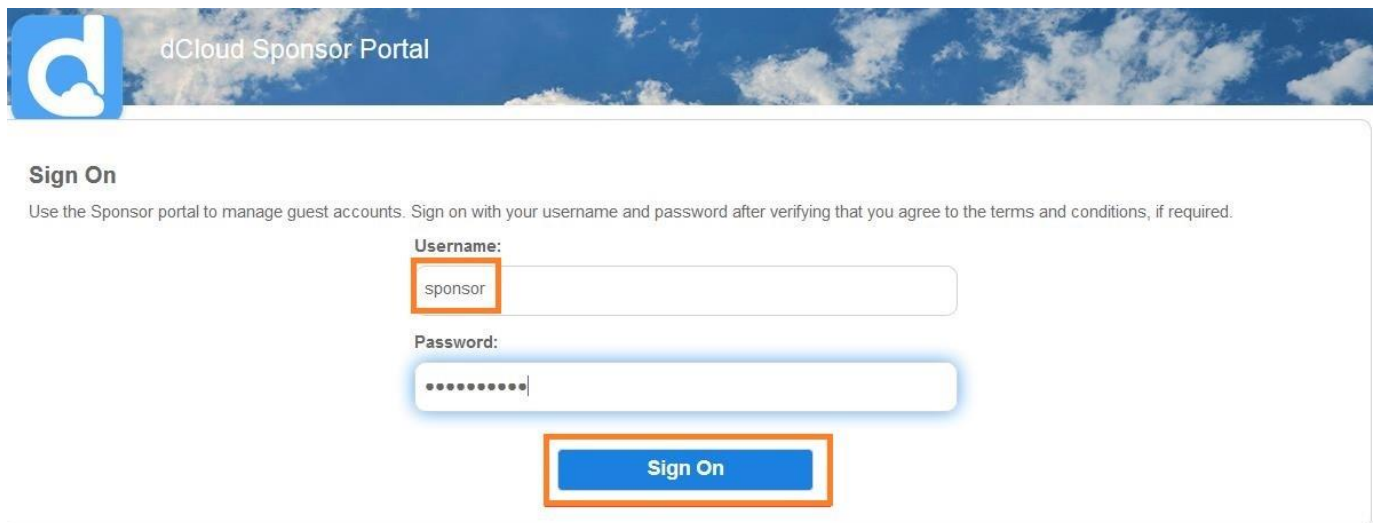
61. **Default Portal Logins** 섹션에서 **Sponsor Portal** 을 클릭하여 스폰서 포털 로그인 페이지로 이동합니다.

그림: 토폴로지 페이지



62. 사용자 ID/패스워드를 **sponsor/C1sco12345** 조합으로 사용하여 **Sponsor Portal** 에 로그인합니다.

그림: 스폰서 포털 로그인 페이지



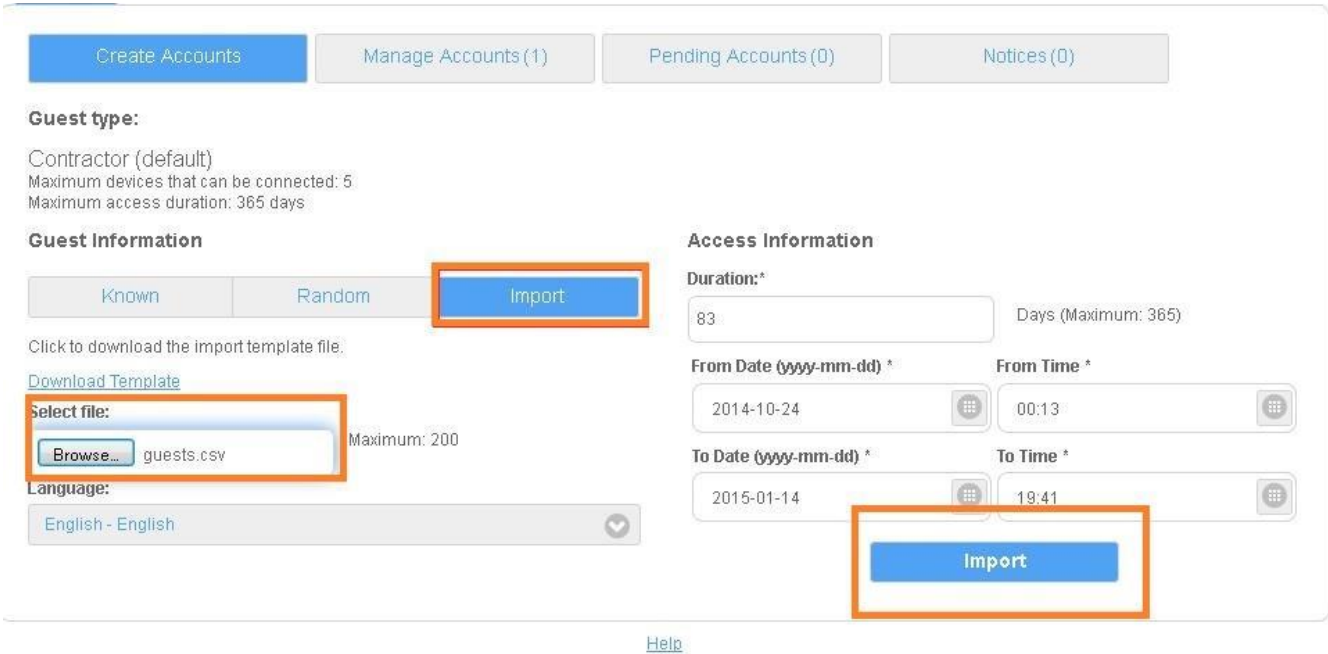
63. **Create Accounts** 탭에서, **Import** 탭을 클릭합니다.

64. **Browse** 를 클릭하고 데스크탑에서 **guest.csv** 파일을 선택합니다.

65. **Open** 을 클릭합니다.

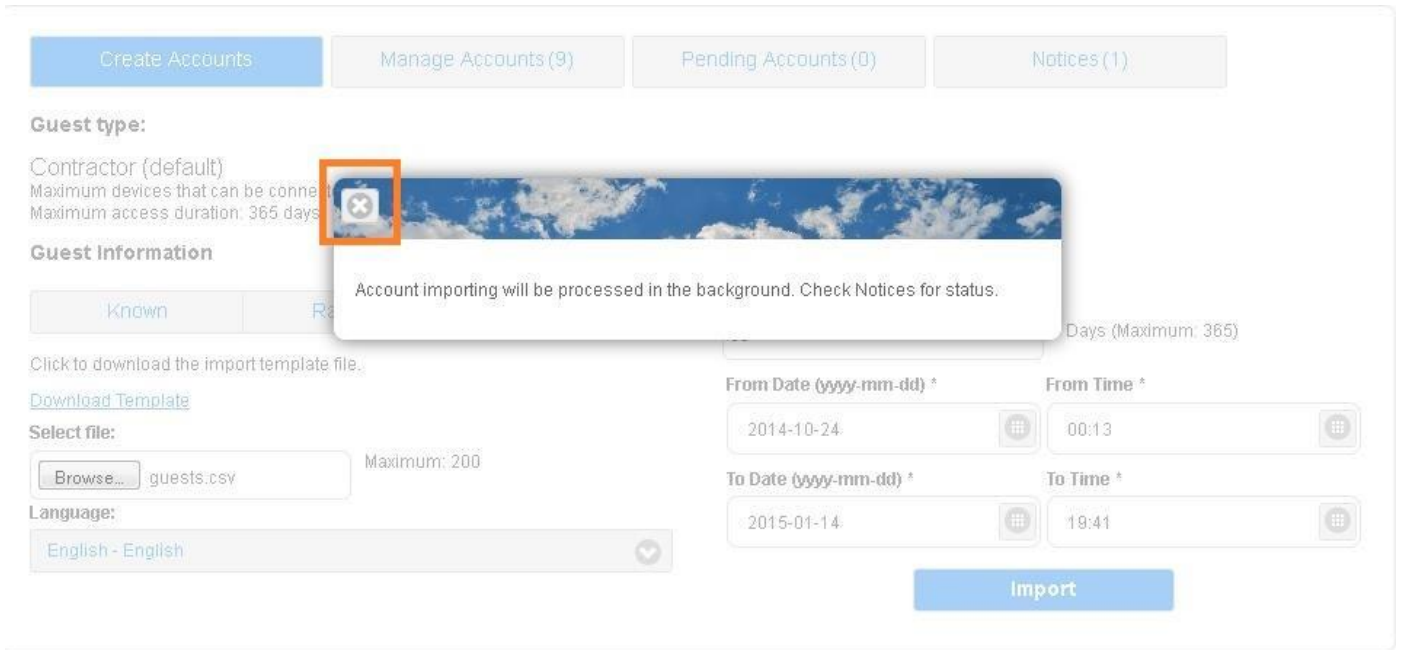
66. 스폰서 포털의 오른쪽 하단에서 **Import** 를 클릭합니다.

그림: 대량 계정 만들기



67. X 를 클릭하여 팝업 창을 닫습니다.

그림: 팝업창 (Pop up Window)



68. Notices 탭을 클릭합니다. 8 개의 계정이 성공적으로 생성되었음을 보여줍니다.

그림: Import Accounts 만들기

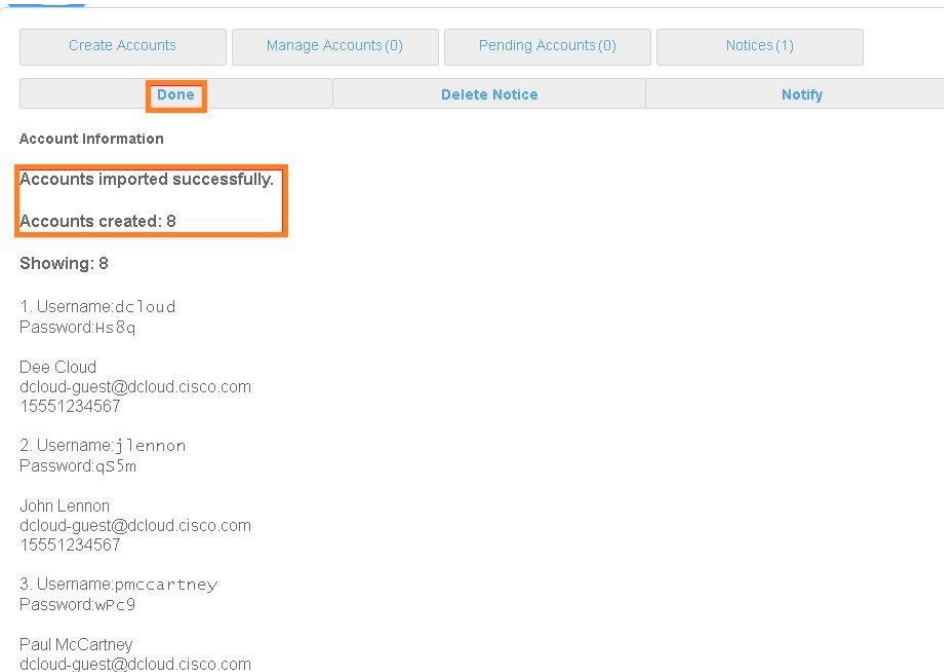


Action Name	Number of Accounts	Status	Start	End
Create Import Accounts	8	Success	2014-10-24T00:16:46.734Z	2014-10-24T00:16:47.909Z

69. **Create Import Accounts** 알림을 클릭하여 알림을 표시합니다. guests.csv 에서 각 사용자에 대한 모든 계정 정보가 포함된 8 개의 사용자 계정이 생성되었습니다.

70. **Done** 을 클릭하여 스폰서 포털 페이지로 돌아갑니다.

그림: 대량 게스트 계정을 성공적으로 가져옴



Account Information

Accounts imported successfully.
Accounts created: 8

Showing: 8

1. Username:dc1oud
Password:Hs8q

Dee Cloud
dcloud-guest@dcloud.cisco.com
15551234567
2. Username:j1ennon
Password:qS5m

John Lennon
dcloud-guest@dcloud.cisco.com
15551234567
3. Username:pmccartney
Password:wPc9

Paul McCartney
dcloud-guest@dcloud.cisco.com

71. **Manage Accounts** 탭을 클릭하여 이전에 생성된 모든 게스트 계정 외에 추가된 8 개의 게스트 계정을 볼 수 있습니다.

그림: Guest Accounts

Create Accounts
Manage Accounts (9)
Pending Accounts (0)
Notices (1)

Edit
Resend
Extend
Suspend
Delete
Reset Password
Reinstate
Refresh

<input type="checkbox"/> User ...	State	First Name	Last Name	Email Ad...	Phone N...	Group Tag	Location	Sponsor	Guest Ty...	Expirati...	Time Left
<input type="checkbox"/> bdylan	Created	Bob	Dylan	dcloud-guest@dcl...	15551234...		London	sponsor	Contractor (default)	2015-01-14 19:41	82D 19H 18M
<input type="checkbox"/> dcloud	Created	Dee	Cloud	dcloud-guest@dcl...	15551234...		London	sponsor	Contractor (default)	2015-01-14 19:41	82D 19H 18M
<input type="checkbox"/> eclapton	Created	Eric	Clapton	dcloud-guest@dcl...	15551234...		London	sponsor	Contractor (default)	2015-01-14 19:41	82D 19H 18M

노트: 사용자의 편의를 위해 **Workstation1** 컴퓨터에 **Open Office Calc** 가 로드되었습니다. 원하는 경우 **guests.csv** 파일을 열어 편집하고 고유한 게스트 계정을 추가할 수 있습니다.



What's Next?

<http://cs.co/selling-ise-demos> 에서 다른 ISE 데모를 확인할 수 있습니다.

[dCloud Community](#) 에서 논의할 수 있습니다.



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)