WLC(Wireless LAN Controller)에서 LDAP를 사용한 웹 인증 컨피그레이션 예

목차

소개

이 문서에서는 웹 인증을 위해 WLC(Wireless LAN Controller)를 설정하는 방법에 대해 설명합니다. 사용자 자격 증명을 검색하고 사용자를 인증하기 위해 웹 인증을 위한 백엔드 데이터베이스로 LDAP(Lightweight Directory Access Protocol) 서버를 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- LAP(Lightweight Access Point) 및 Cisco WLC 구성에 대한 지식
- CAPWAP(Control And Provisioning of Wireless Access Point Protocol) 지식
- LDAP(Lightweight Directory Access Protocol), Active Directory 및 도메인 컨트롤러를 설정 및 구성하는 방법에 대한 지식

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 펌웨어 릴리스 8.2.100.0을 실행하는 Cisco 5508 WLC
- Cisco 1142 Series LAP
- Cisco 802.11a/b/g 무선 클라이언트 어댑터.
- LDAP 서버의 역할을 수행하는 Microsoft Windows 2012 Essentials 서버

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

표기 규칙

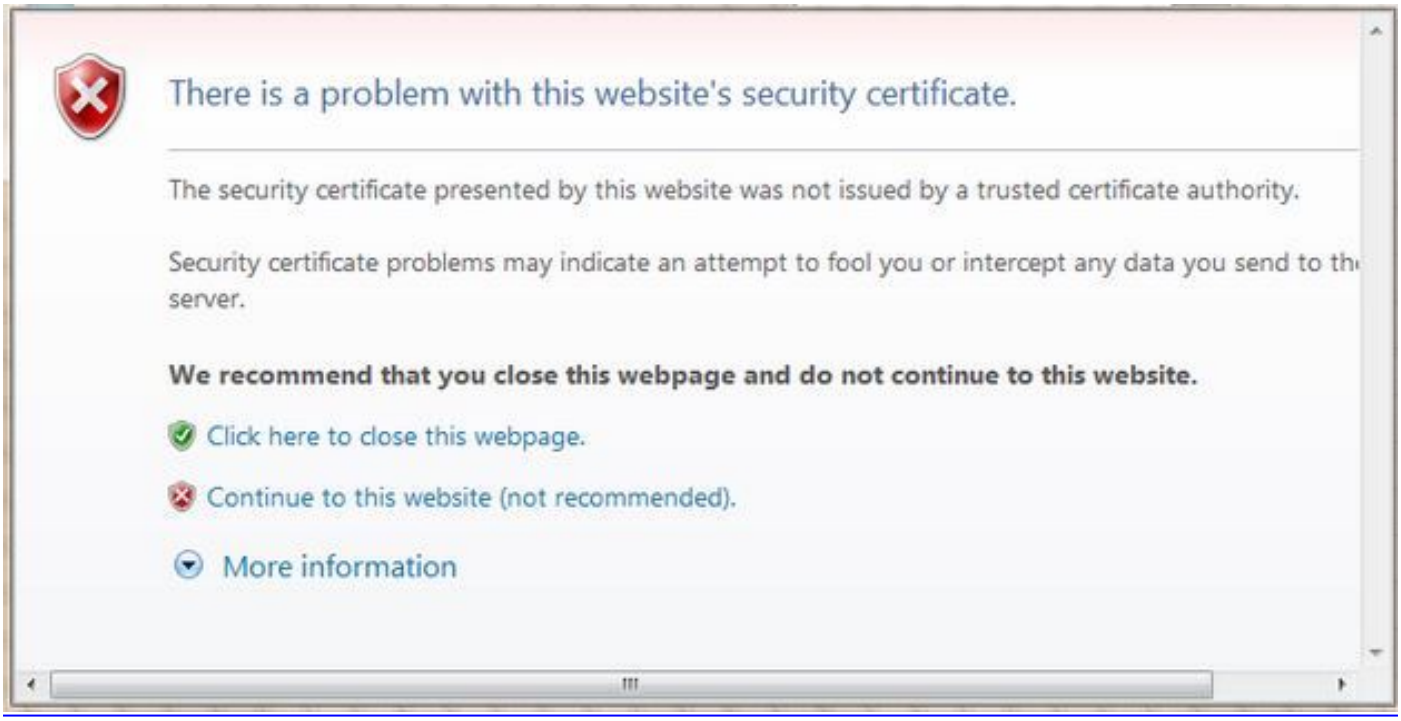
문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참조하십시오.

웹 인증 프로세스

웹 인증은 레이어 3 보안 기능으로, 클라이언트가 올바른 사용자 이름과 비밀번호를 제공할 때까지 컨트롤러가 특정 클라이언트의 IP 트래픽(DHCP 및 DNS 관련 패킷 제외)을 허용하지 않습니다. 웹 인증을 사용하여 클라이언트를 인증하는 경우 각 클라이언트에 대한 사용자 이름 및 비밀번호를 정의해야 합니다. 그런 다음 클라이언트가 무선 LAN에 가입하려고 할 때 로그인 페이지에서 사용자 이름과 비밀번호를 입력해야 합니다.

레이어 3 보안 아래에서 웹 인증이 활성화되면 사용자가 URL에 처음 액세스하려고 할 때 웹 브라우저 보안 알림을 수신하는 경우가 있습니다.

> **팁**: 이 인증서 경고를 제거하려면 신뢰할 수 있는 서드파티 인증서를 설치하는 방법에 대한 다음 설명서로 되돌아가십시오http://www.cisco.com/c/en/us/support/docs/wireless/4400-series-wireless-lan-controllers/109597-csr-chained-certificates-wlc-00.html

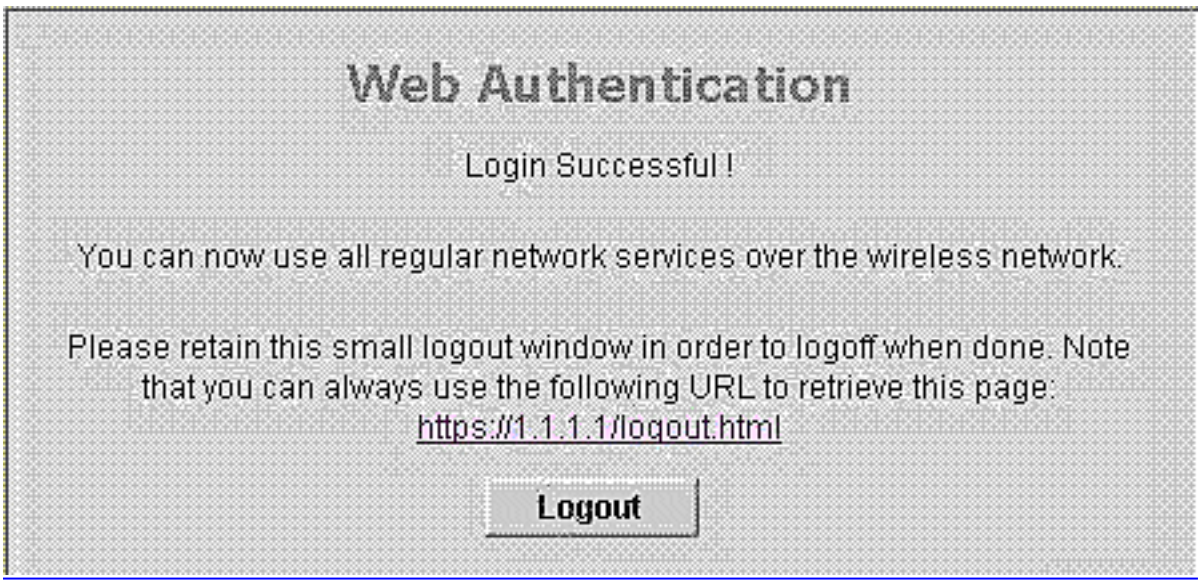


예를 클릭하여 계속 진행하거나 Firefox 브라우저**의** 경우 **이 웹 사이트**로 계속**(예**를 들어 **권장 안 함**) 또는 클라이언트의 브라우저에 보안 알림이 표시되지 않으면 웹 인증 시스템은 이미지에 표시된 대로 클라이언트를 로그인 페이지로 리디렉션합니다.

기본 로그인 페이지에는 Cisco 로고 및 Cisco 관련 텍스트가 포함되어 있습니다. 웹 인증 시스템에서 다음 중 하나를 표시하도록 선택할 수 있습니다.

- 기본 로그인 페이지
- 기본 로그인 페이지의 수정된 버전
- 외부 웹 서버에서 구성하는 사용자 지정 로그인 페이지
- 컨트롤러에 다운로드하는 사용자 지정 로그인 페이지

웹 인증 로그인 페이지에서 유효한 사용자 이름 및 비밀번호를 입력하고 Submit(제출)을 클릭하면, 제출된 자격 증명과 백엔드 데이터베이스(이 경우 LDAP)의 성공적인 인증에 따라 인증됩니다. 그런 다음 웹 인증 시스템은 성공 적 인 로그인 페이지를 표시 하고 요청 한 URL로 인증 된 클라이언트를 재전송 합니다.



기본 성공 로그인 페이지에는 가상 게이트웨이 주소 URL(https://1.1.1.1/logout.html)에 대한 포인터가 있습니다. 컨트롤러 가상 인터페이스에 대해 설정한 IP 주소는 로그인 페이지의 리디렉션 주소 역할을 합니다.

이 문서에서는 웹 인증에 WLC의 내부 웹 페이지를 사용하는 방법에 대해 설명합니다. 이 예에서는 사용자 자격 증명을 검색하고 사용자를 인증하기 위해 웹 인증을 위한 백엔드 데이터베이스로 LDAP 서버를 사용합니다.

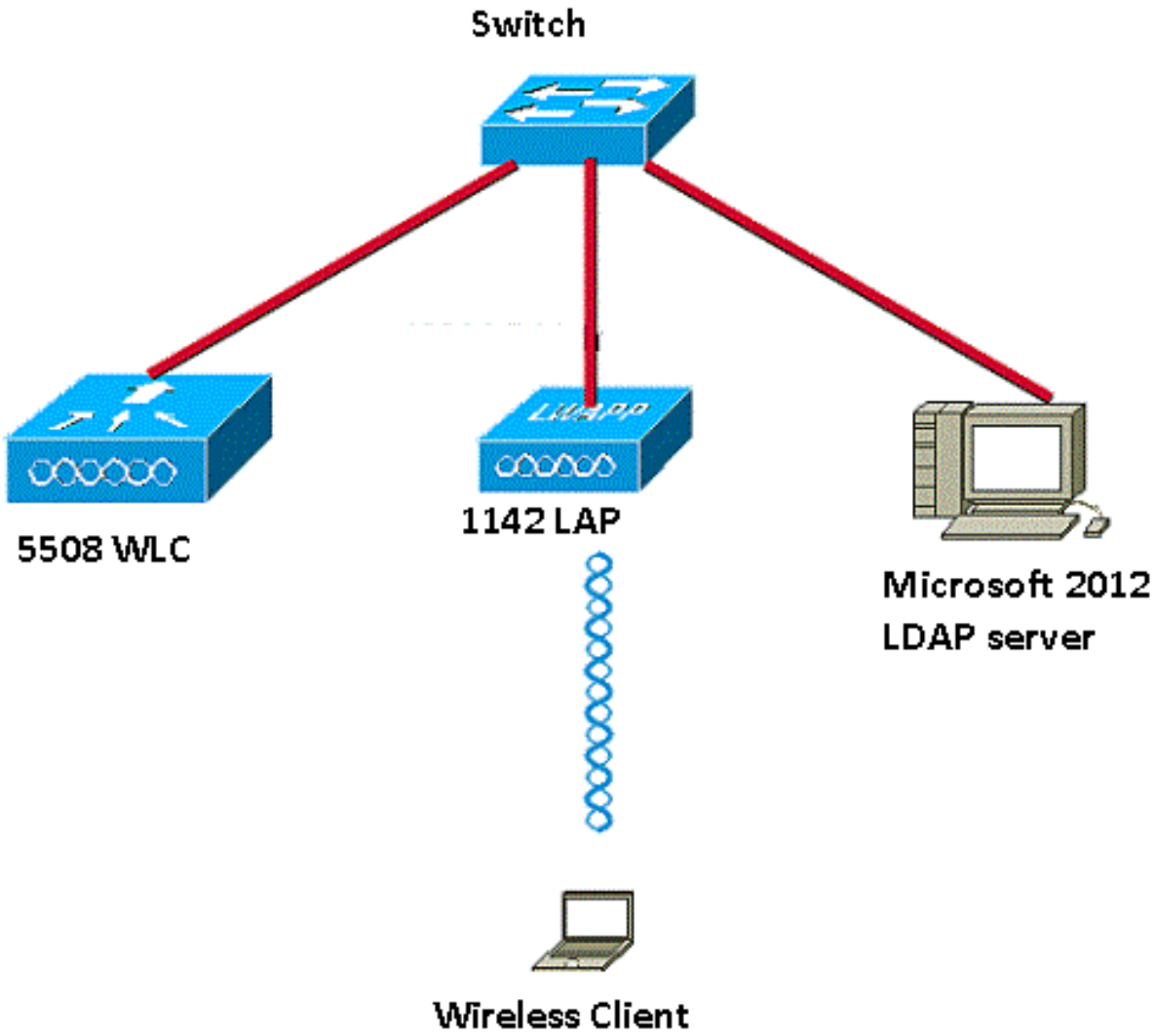
구성

이 섹션에는 이 문서에서 설명하는 기능을 구성하기 위한 정보가 표시됩니다.

> **참고**: 이 섹션에서 사용된 명령에 대한 자세한 내용을 보려면 명령 조회 툴(등록된 고객만 해당)을 사용하십시오.

네트워크 다이어그램

이 문서에서는 이 네트워크 설정을 사용합니다.



설정

이 설정을 성공적으로 구현하려면 다음 단계를 완료하십시오.

- LDAP 서버를 구성합니다.
- LDAP 서버에 대한 WLC를 구성합니다.
- 웹 인증을 위해 WLAN을 구성합니다.

LDAP 서버 구성

첫 번째 단계는 LDAP 서버를 구성하는 것입니다. 이 서버는 무선 클라이언트의 사용자 자격 증명을 저장하는 백엔드 데이터베이스 역할을 합니다. 이 예에서는 Microsoft Windows 2012 Essentials 서버가 LDAP 서버로 사용됩니다.

LDAP 서버 컨피그레이션의 첫 번째 단계는 WLC가 이 데이터베이스에 쿼리하여 사용자를 인증할 수 있도록 LDAP 서버에 사용자 데이터베이스를 만드는 것입니다.

도메인 컨트롤러에서 사용자 생성

OU(조직 구성 단위)에는 PersonProfile의 개인 항목에 대한 참조를 전달하는 여러 그룹이 포함되어 있습니다. 한 사람이 여러 그룹의 구성원이 될 수 있습니다. 모든 객체 클래스 및 속성 정의는 LDAP 스키마 기본값입니다. 각 그룹에는 해당 그룹에 속한 각 사용자에 대한 참조(dn)가 포함되어 있습니

다.

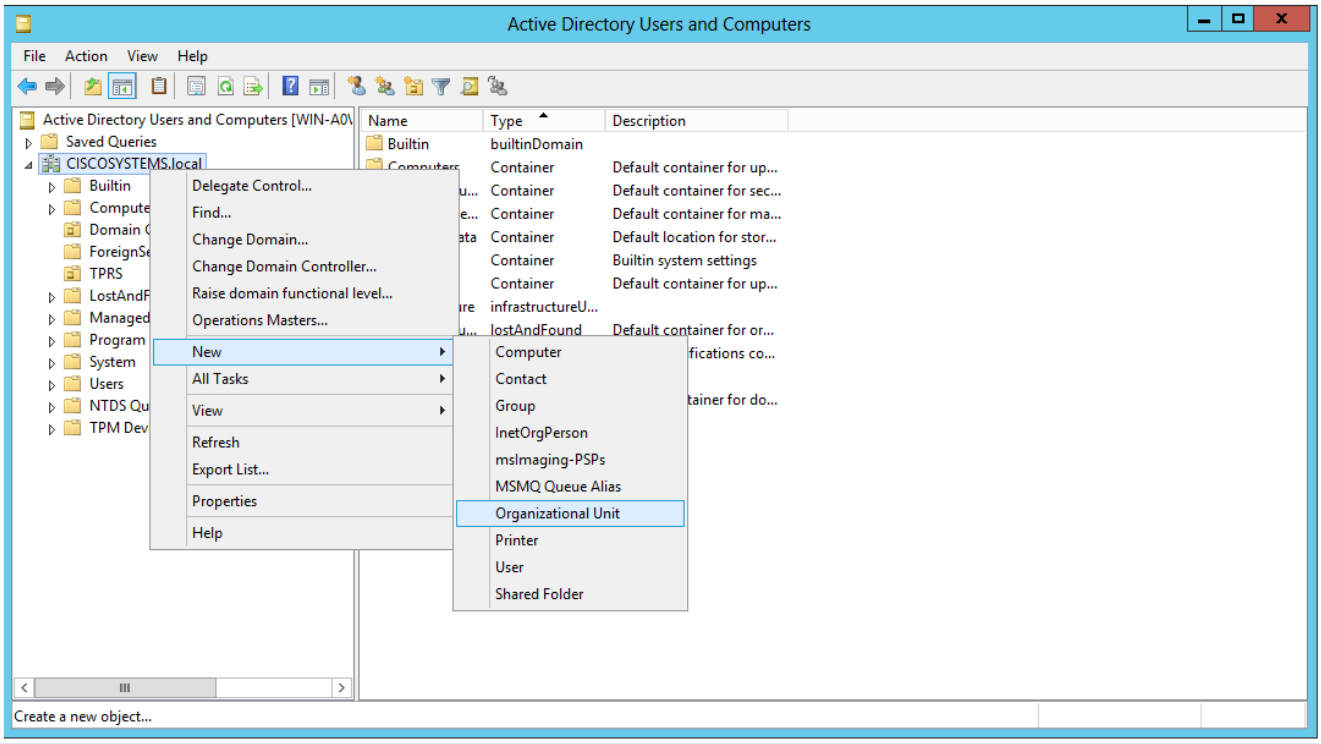
이 예에서는 새 OU LDAP-USERS가 생성되고 사용자 User1이 이 OU 아래에 생성됩니다. LDAP 액세스를 위해 이 사용자를 구성할 때 WLC는 사용자 인증을 위해 이 LDAP 데이터베이스에 쿼리할 수 있습니다.

이 예에서 사용되는 도메인은 **CISCOSYSTEMS.local입니다**.

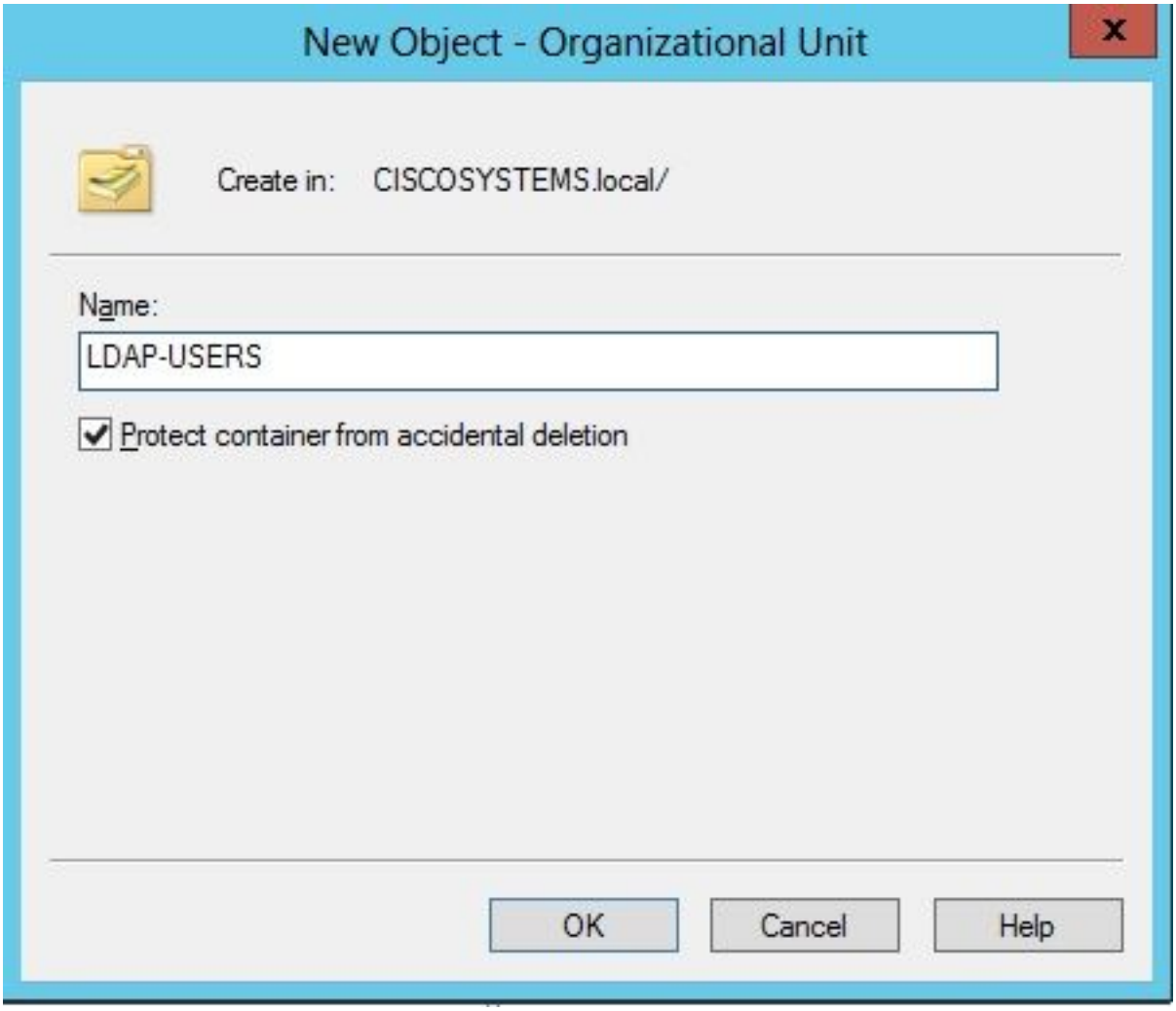
OU에서 사용자 데이터베이스 만들기

이 섹션에서는 도메인에 새 OU를 만들고 이 OU에 새 사용자를 만드는 방법에 대해 설명합니다.

1. Windows PowerShell을 열고 servermanager**.exe를 입력합니다.**
2. 서버 관리자 창에서 **AD DS**를 클릭합니다**.** 그런 다음 서버 이름을 마우스 오른쪽 단추로 클릭하여 **Active Directory 사용자 및 컴퓨터를** 선택합니다**.**
3. 이 예에서 CISCOSYSTEMS**.local**인 도메인 이름을 마우스 오른쪽 버튼으로 클릭한 다음 컨텍스트 메뉴에서 **New > Organizational Unit**으로 이동하여 새 OU를 만듭니다.

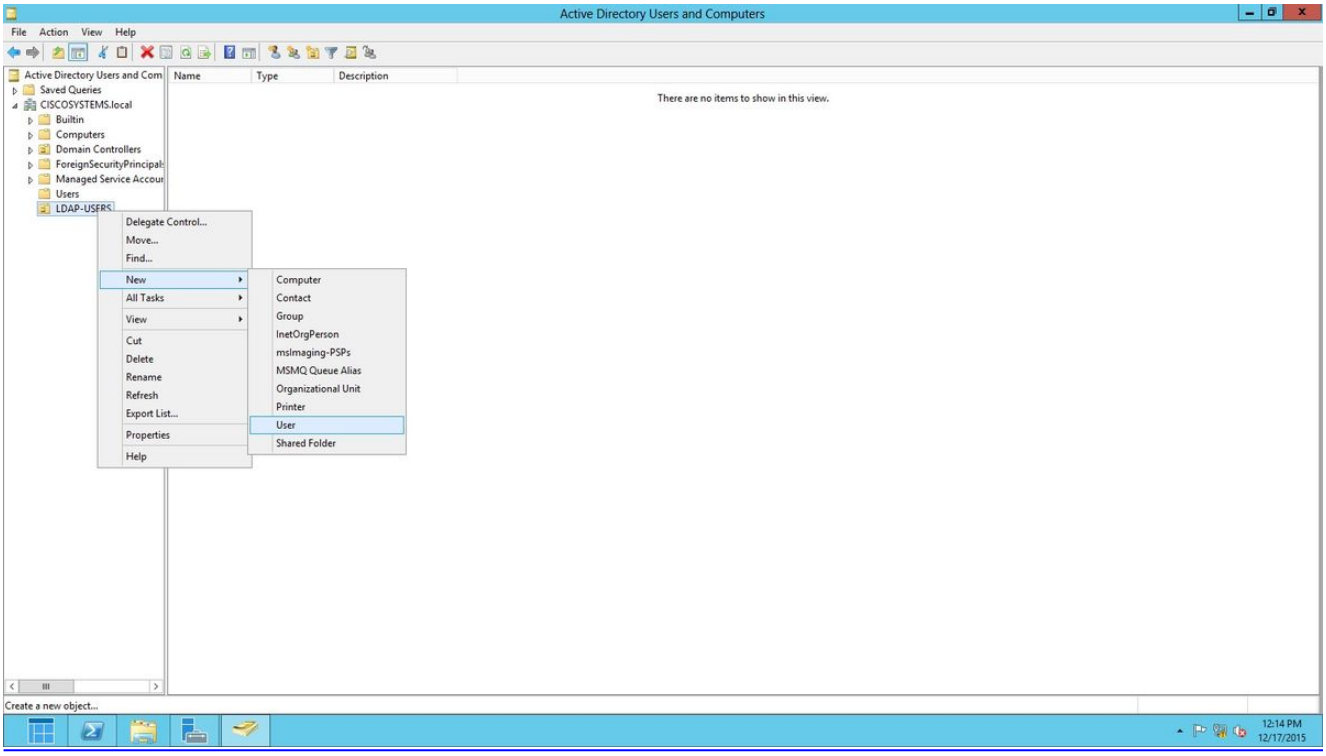


4. 이미지에 표시된 대로 이 OU에 이름을 지정하고 **OK**(확인)를 클릭합니다.



이제 LDAP 서버에 새 OU LDAP-USERS가 생성되었으므로 다음 단계는 이 OU 아래에 user **User1**을 생성하는 것입니다. 이를 위해 다음 단계를 완료하십시오.

1. 생성된 새 OU를 마우스 오른쪽 버튼으로 클릭합니다. 이미지에 표시된 대로 새 **사용자를** 생성하기 위해 결과 컨텍스트 메뉴에서 LDAP-USERS**> New > User**로 이동합니다.

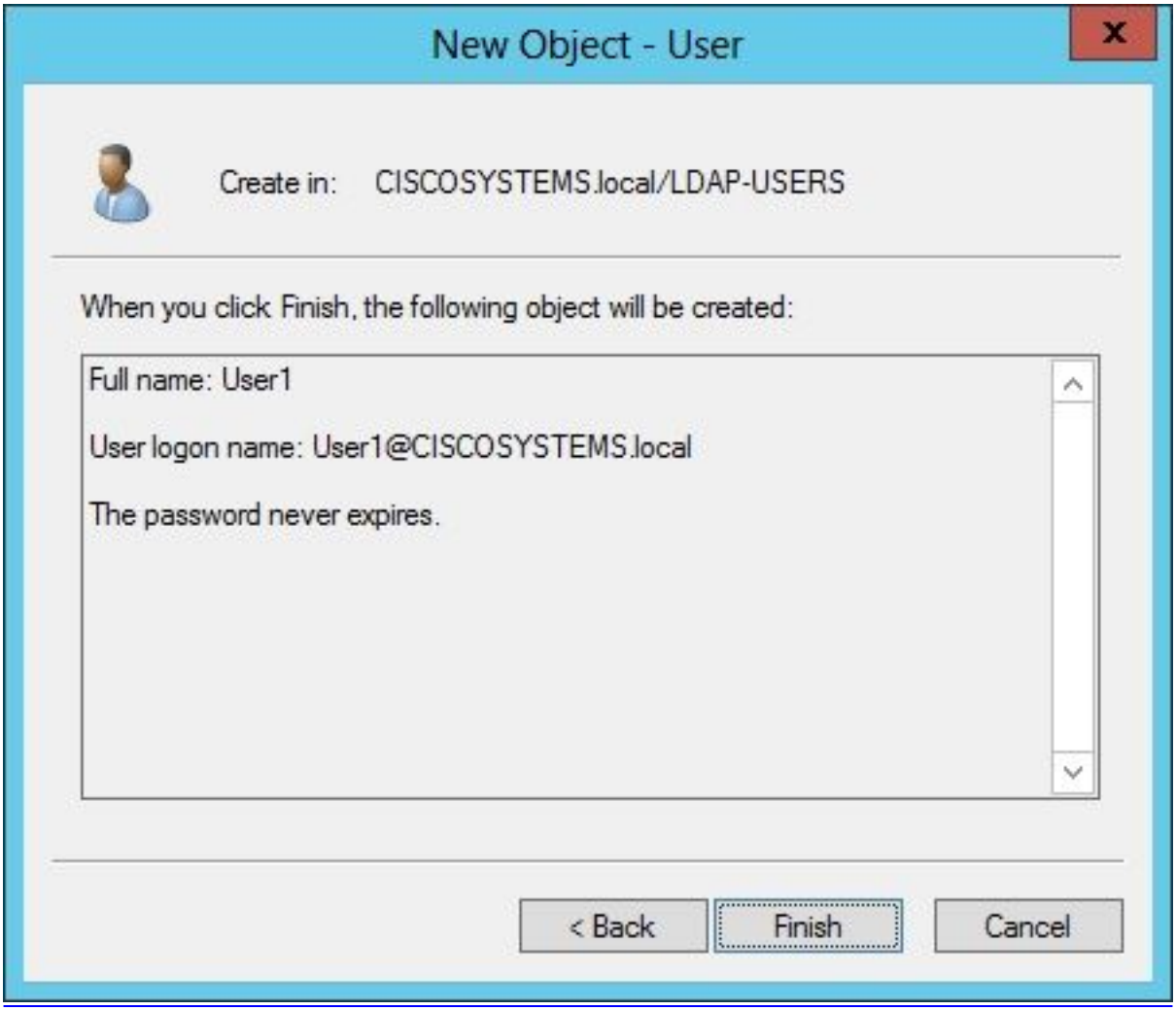


2. User setup(사용자 설정) 페이지에서 이 예에 표시된 대로 필수 필드를 입력합니다. 이 예에서는 User **logon name** 필드에 **User1이** 있습니다.클라이언트를 인증하기 위해 LDAP 데이터베이스에서 확인되는 사용자 이름입니다. 이 예에서는 First name 및 Full Name 필드에 User1을 사용합니다. **Next(다음)**를 클릭합니다.

3. 비밀번호를 입력하고 비밀번호를 확인합니다. Password never expires(**비밀번호 만료되지 않**

음) 옵션을 선택하고 Next(**다음)**를 클릭합니다.

4. **Finish(마침)**를 클릭합니다.OU LDAP-USERS 아래에 새 사용자 User1이 생성됩니다. 다음은 사용자 자격 증명입니다.사용자 이름: **User1**암호: **랩톱123**



이제 사용자가 OU에서 생성되었으므로 다음 단계는 LDAP 액세스를 위해 이 사용자를 구성하는 것입니다.

LDAP 액세스를 위한 사용자 구성

LDAP 서버에 대한 로컬 인증 **바인딩** 방법을 **지정하려면 Anonymous**(익명) 또는 Authenticated(인증됨)를 선택할 수 있습니다. Anonymous 메서드는 LDAP 서버에 대한 익명 액세스를 허용합니다. Authenticated(인증된) 방법을 사용하려면 보안 액세스를 위해 사용자 이름 및 비밀번호를 입력해야 합니다. 기본값은 Anonymous입니다.

이 섹션에서는 익명 및 인증 방법을 모두 구성하는 방법에 대해 설명합니다.

익명 바인딩

참고: 익명 바인딩을 사용하지 않는 것이 좋습니다. LDAP . Anonymous bind LDAP .

LDAP 액세스를 위한 익명 사용자를 구성하려면 이 섹션의 단계를 수행합니다.

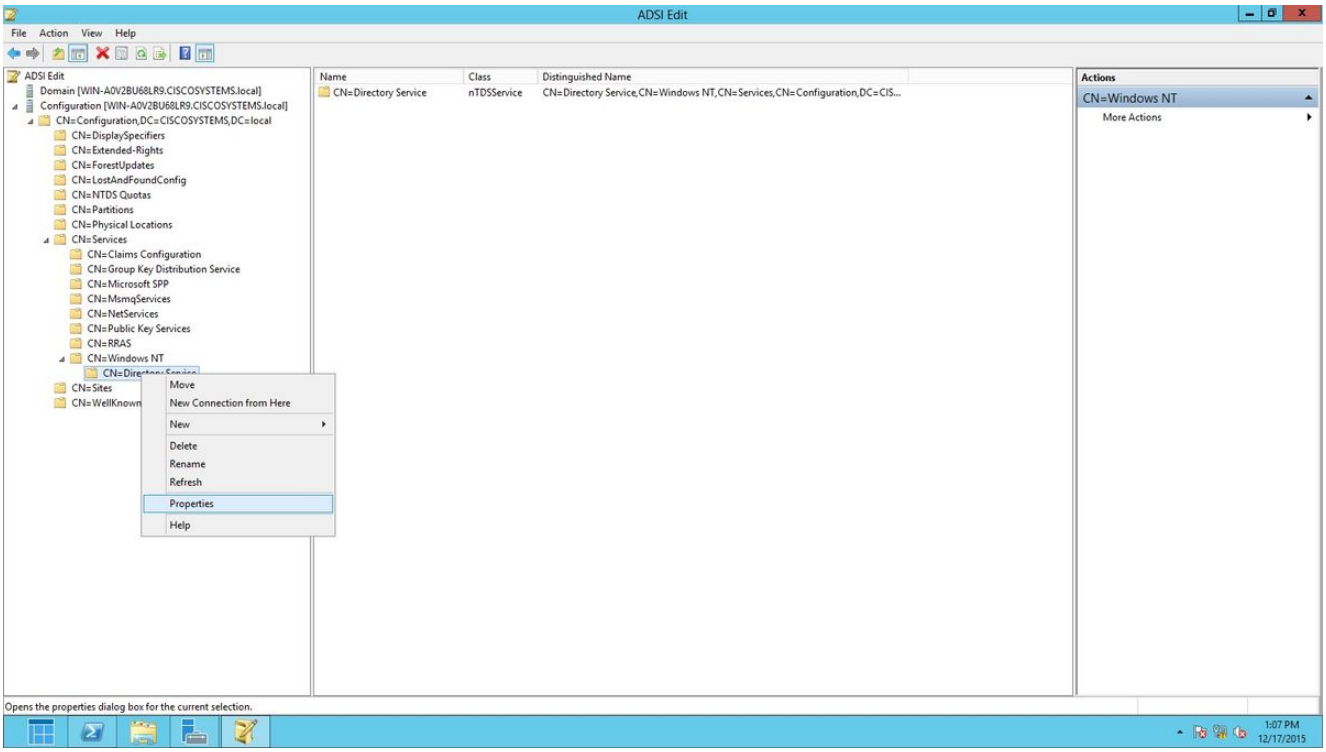
Windows 2012 Essentials 서버에서 익명 바인딩 기능 사용

서드파티 애플리케이션(여기서는 WLC)이 LDAP에서 Windows 2012 AD에 액세스하려면 Windows 2012에서 익명 바인딩 기능을 활성화해야 합니다. 기본적으로 Windows 2012 도메인 컨트롤러에서는 익명 LDAP 작업이 허용되지 않습니다. 익명 바인딩 기능을 활성화하려면 다음 단계를 수행합니

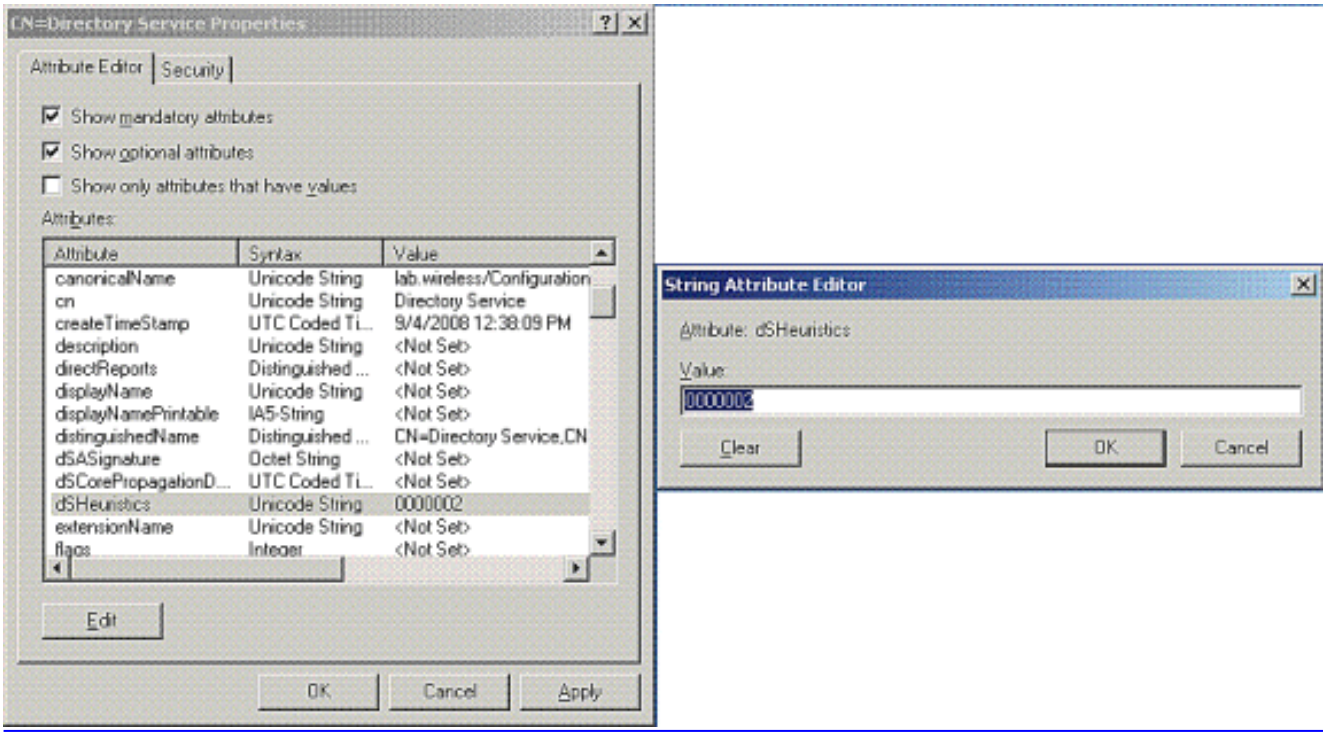
다.

1. Windows PowerShell에 ADSIEdit.msc를 입력하여 **ADSI 편집** 도구를 시작합니다. 이 도구는 Windows 2012 지원 도구의 일부입니다.

2. ADSI Edit(ADSI 편집) 창에서 루트 도메인을 확장합니다(Configuration [WIN-A0V2BU68LR9.CISCOSYSTEMS.local]).**CN=Services > CN=Windows NT > CN=Directory Service로** 이동합니다. 이미지에 표시된 대로 **CN=Directory Service** 컨테이너를 마우스 오른쪽 버튼으로 클릭하고 컨텍스트 메뉴에서 **Properties**(속성)를 선택합니다.



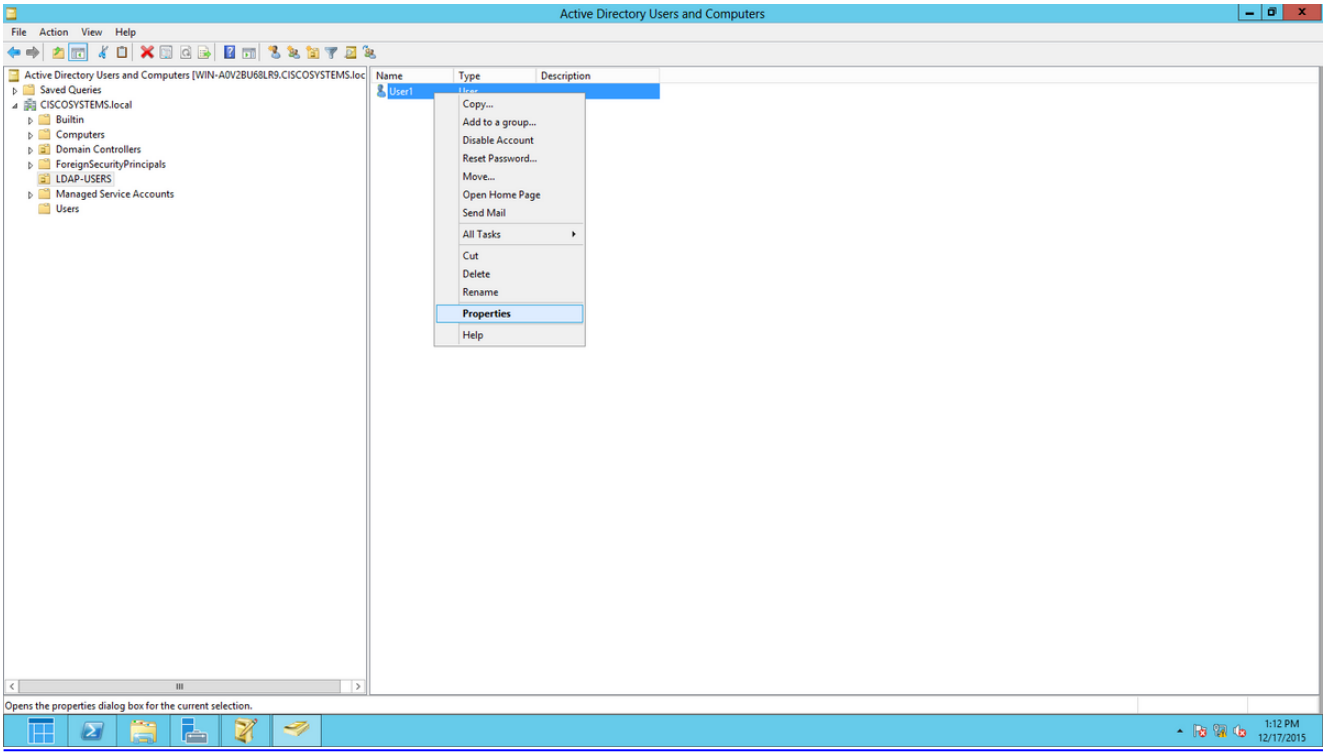
3. CN=Directory Service Properties(CN=디렉토리 서비스 속성) 창의 Attributes(**특성)**에서 Attribute(특성) 필드 **아래**의 dsHeuristics(dsHeuristics) 특성을 클릭하고 Edit(편집)**를 선택합니다**. 이 속성의 String Attribute Editor(문자열 속성 편집기) 창에 값 **000002**를 입력합니다. 그림과 같이 **Apply(적용)** 및 **OK(확인)**를 클릭합니다. 익명 바인딩 기능은 Windows 2012 서버에서 활성화되어 있습니다.**참고**: 마지막(7번째) 문자는 LDAP 서비스에 바인딩할 수 있는 방법을 제어하는 문자입니다. 0(영) 또는 7번째 문자가 없으면 익명 LDAP 작업이 비활성화됨을 의미합니다. 일곱 번째 문자를 2로 설정하면 익명 바인딩 기능이 활성화됩니다
.



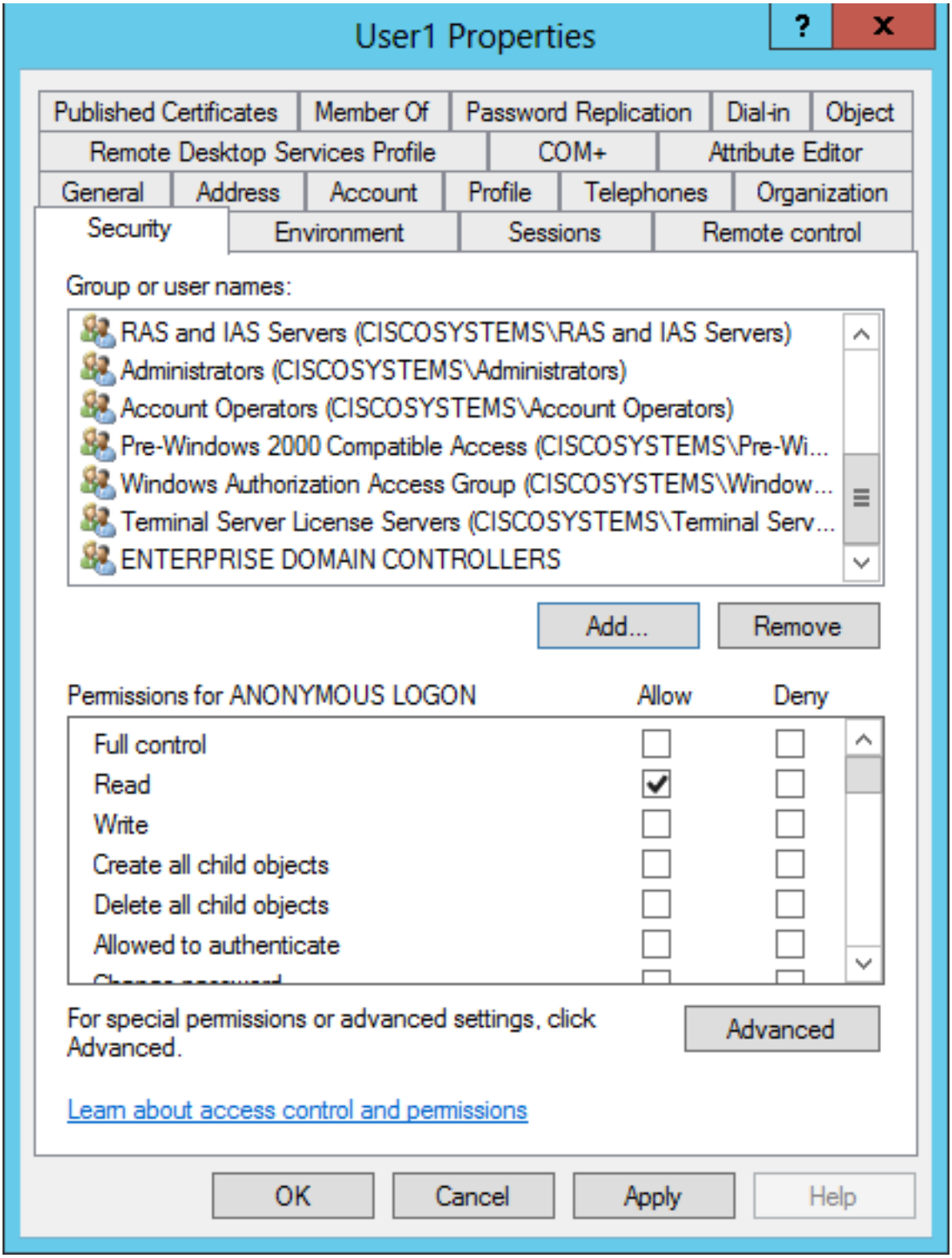
사용자에게 익명 로그온 액세스 권한 부여

다음 단계는 사용자 User1에게 ANONYMOUS LOGON 액세스 권한을 부여하는 것입니다. 이를 위해 다음 단계를 완료하십시오.

1. **Active Directory 사용자 및 컴퓨터를** 엽니다.
2. View **Advanced** Features(**고급 기능 보기)가** 선택되어 있는지 확인합니다.
3. 사용자 User1로 이동하여 마우스 오른쪽 버튼을 클릭합니다. 컨텍스트 **메뉴**에서 속성을 선택합니다. 이 사용자는 이름 User1로 식별됩니다.

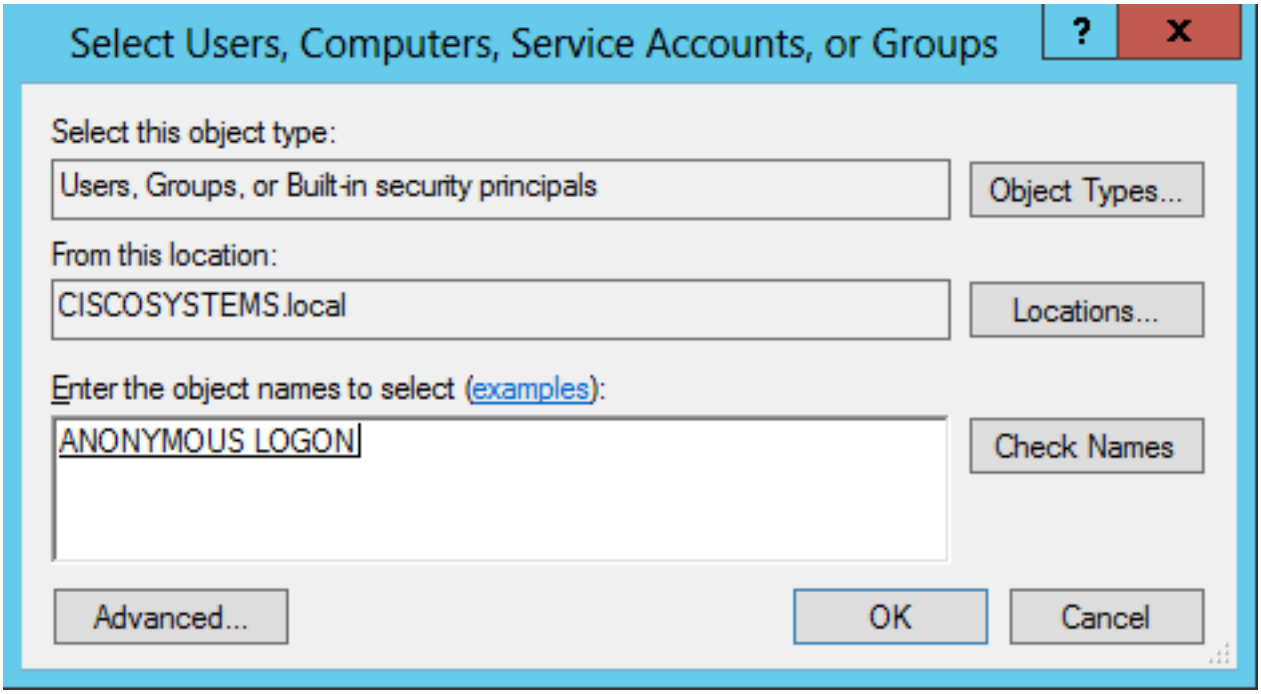


4. 이미지에 표시된 대로 **Security**(보안) 탭을 클릭합니다.

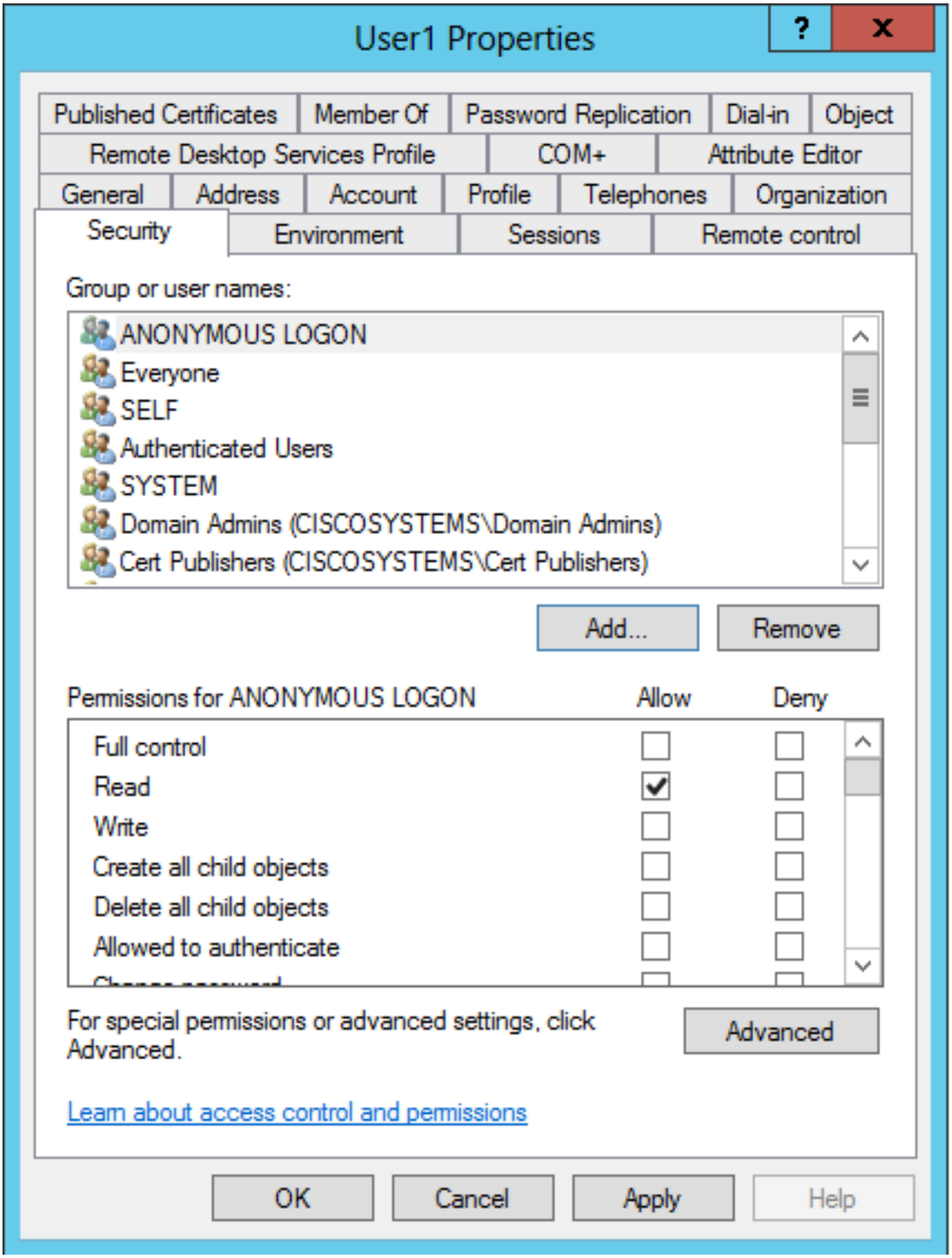


5. 결과 **창**에서 Add를 클릭합니다.

6. 이미지**와** 같이 선택할 *개체 이름 입력 상자*에 ANONYMOUS LOGON을 입력하고 대화 상자를 승인합니다.



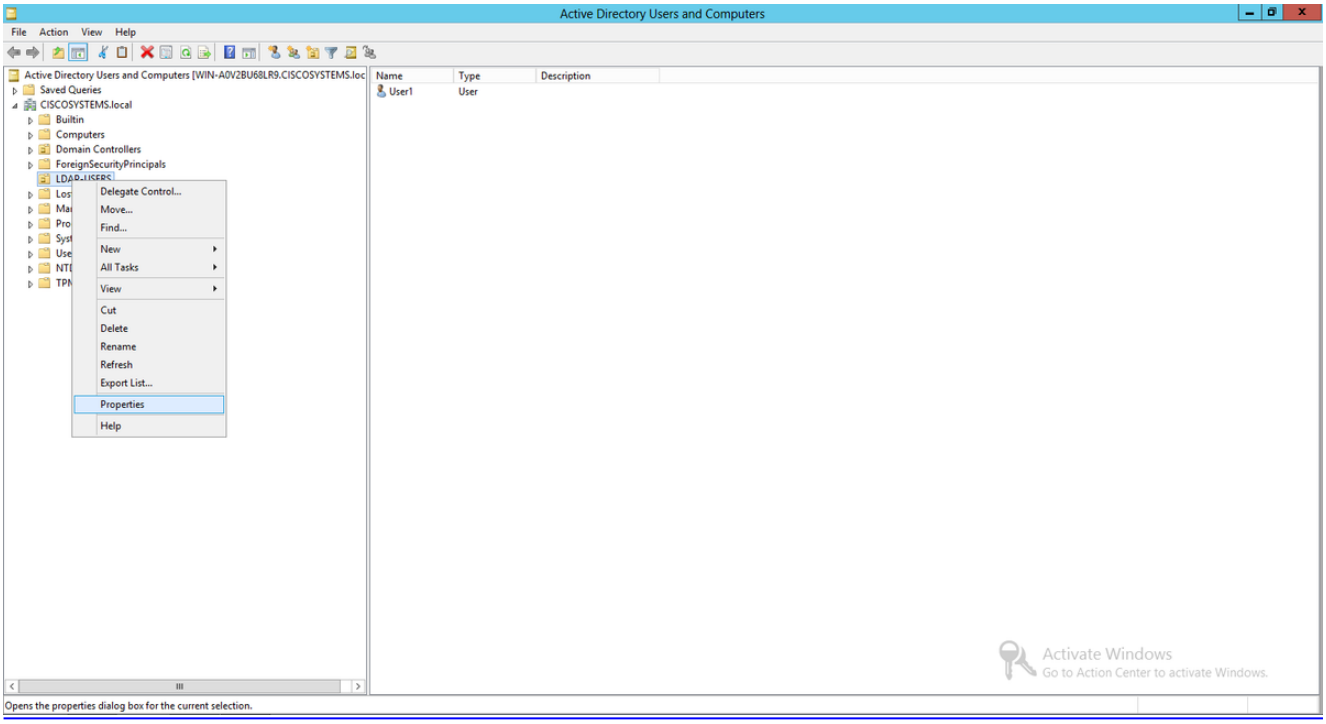
7. ACL에서 ANONYMOUS LOGON은 사용자의 일부 속성 집합에 액세스할 수 있습니다. **OK(확인)**를 클릭합니다. 이미지에 표시된 대로 이 사용자에게 ANONYMOUS LOGON 액세스가 부여됩니다.



OU에 대한 목록 콘텐츠 권한 부여

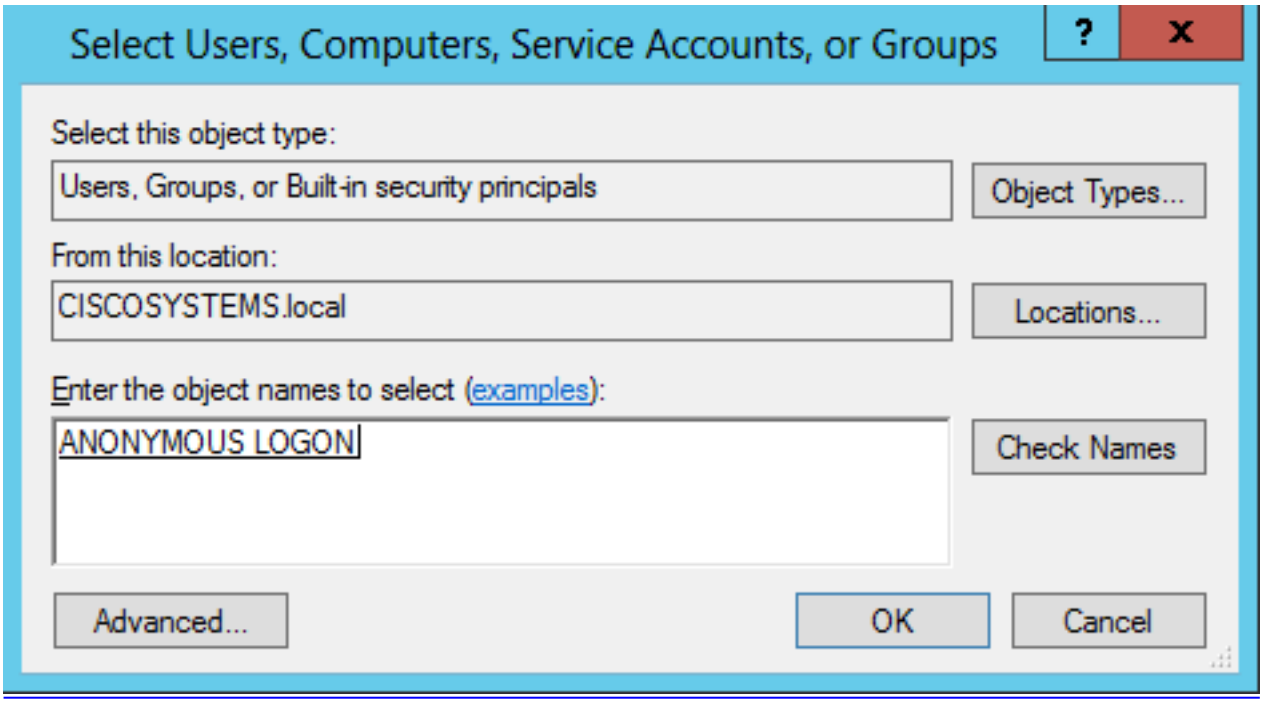
다음 단계는 사용자가 있는 OU의 ANONYMOUS LOGON에 최소한 목록 콘텐츠 사용 권한을 부여하는 것입니다. 이 예에서 User1은 OU LDAP-USERS에 있습니다. 이를 위해 다음 단계를 완료하십시오.

1. 이미지와 같이 **Active Directory Users and Computers(Active Directory 사용자 및 컴퓨터)**에서 **OU LDAP-USERS(OU LDAP-사용자)**를 마우스 오른쪽 버튼으로 클릭하고 **Properties(속성)**를 선택합니다.



2. 보안을 **클릭합니다**.

3. **Add(추가)**를 클릭합니다. 열려 있는 대화 상자에서 이미지에 표시된 대로 **ANONYMOUS** LOGON 및 Acknowledge 대화 상자를 입력합니다.



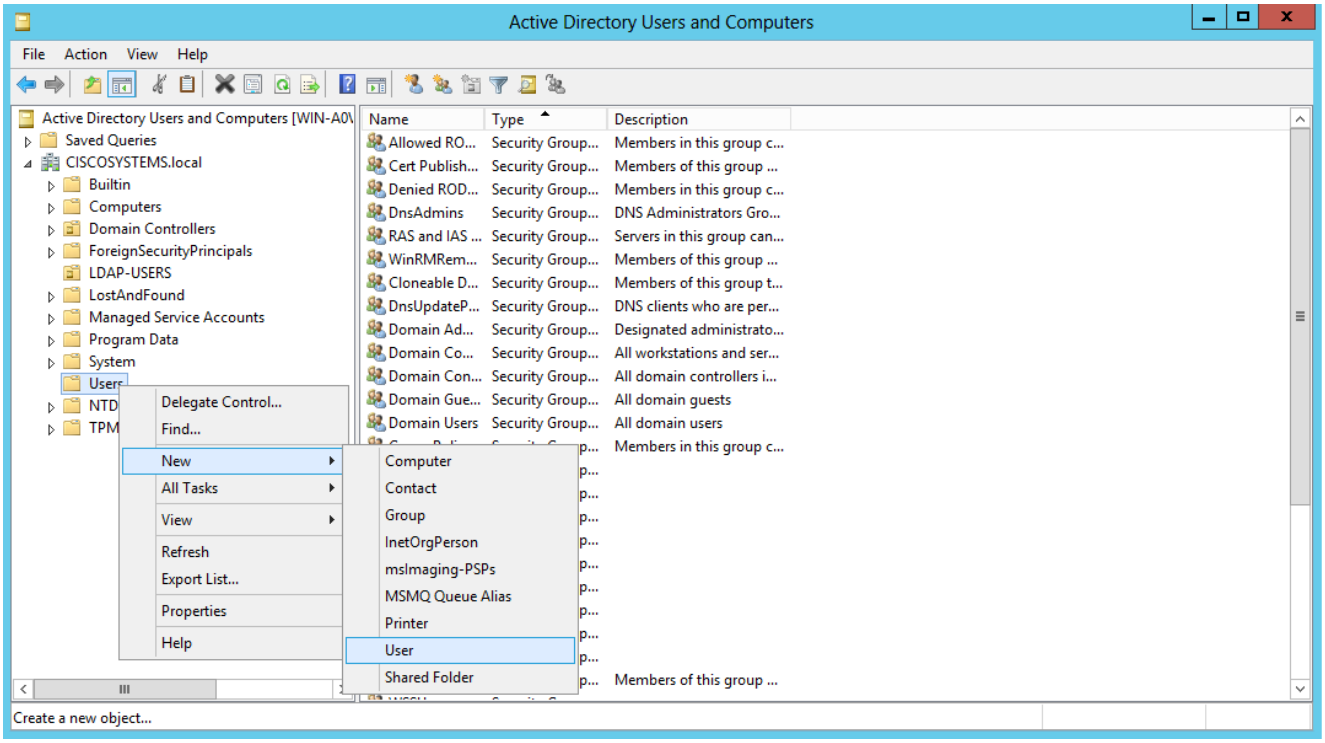
인증된 바인딩

LDAP 서버에 대한 로컬 인증을 위해 사용자를 구성하려면 이 섹션의 단계를 수행합니다.

1. Windows PowerShell을 열고 다음을 입력하십시오. **servermanager.exe**

2. 서버 관리자 창에서 **AD DS**를 클릭합니다. 그런 다음 서버 이름을 마우스 오른쪽 버튼으로 클릭하여 선택합니다 **Active Directory 사용자 및 컴퓨터.**

3. 사용자를 마우스 오른쪽 버튼**으로 클릭합니다**. 결과 컨텍스트 메뉴에서 **새로 만들기 > 사용자**로 이동하여 새 사용자를 생성합니다.



4. User setup(사용자 설정) 페이지에서 이 예에 표시된 대로 필수 필드를 입력합니다. 이 예에서는 **User logon name(사용자 로그온 이름)** 필드에 **WLC-admin이** 있습니다. LDAP 서버에 대한 로컬 인증에 사용할 사용자 이름입니다. **Next(다음)**를 클릭합니다.

5. 비밀번호를 입력하고 비밀번호를 확인합니다. Password never expires(**비밀번호 만료되지 않음) 옵션**을 선택하고 Next(**다음)**를 클릭합니다.

6. **Finish(마침)**를 클릭합니다.사용자 컨테이너 아래에 새 사용자 WLC-admin**이** 생성됩니다. 다음은 사용자 자격 증명입니다.사용자 이름: **WLC-admin**비밀번호: **Admin123**

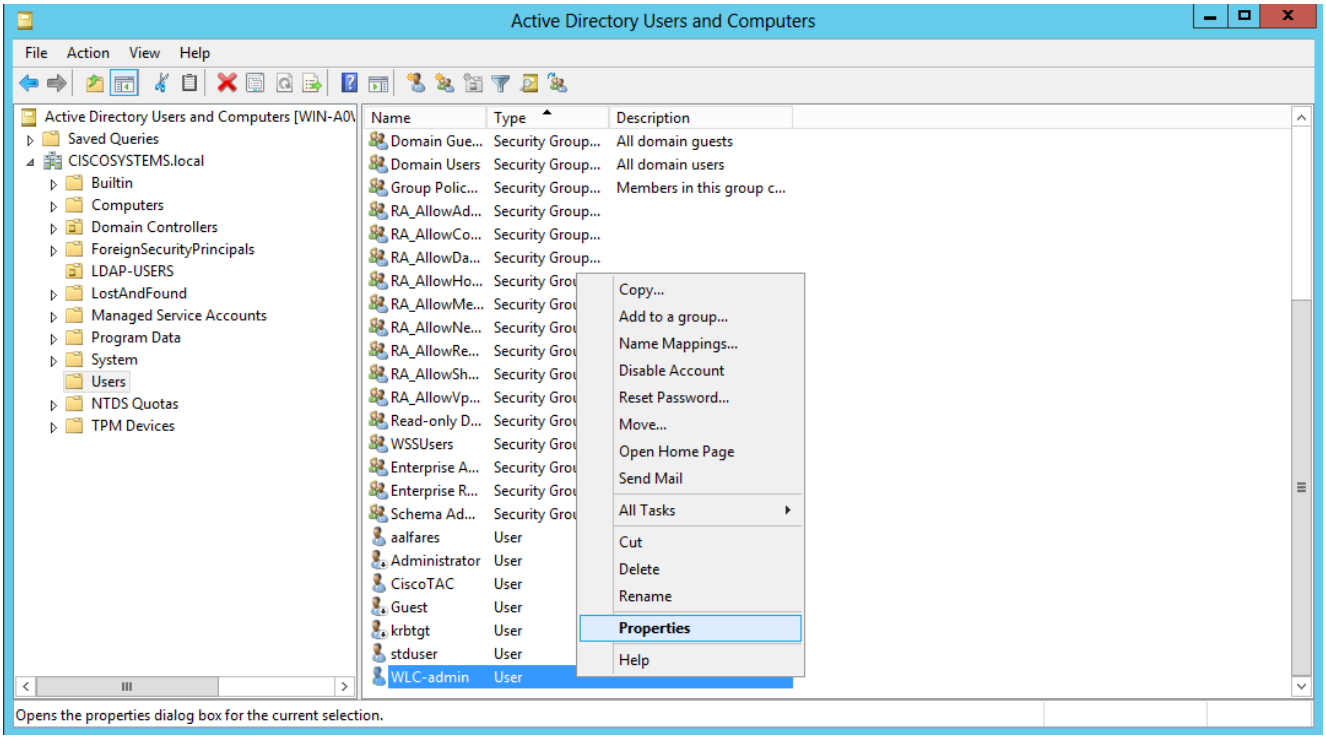
WLC 관리자에게 관리자 권한 부여

이제 로컬 인증 사용자가 생성되었으므로 Administrator 권한을 부여해야 합니다. 이를 위해 다음 단계를 완료하십시오.

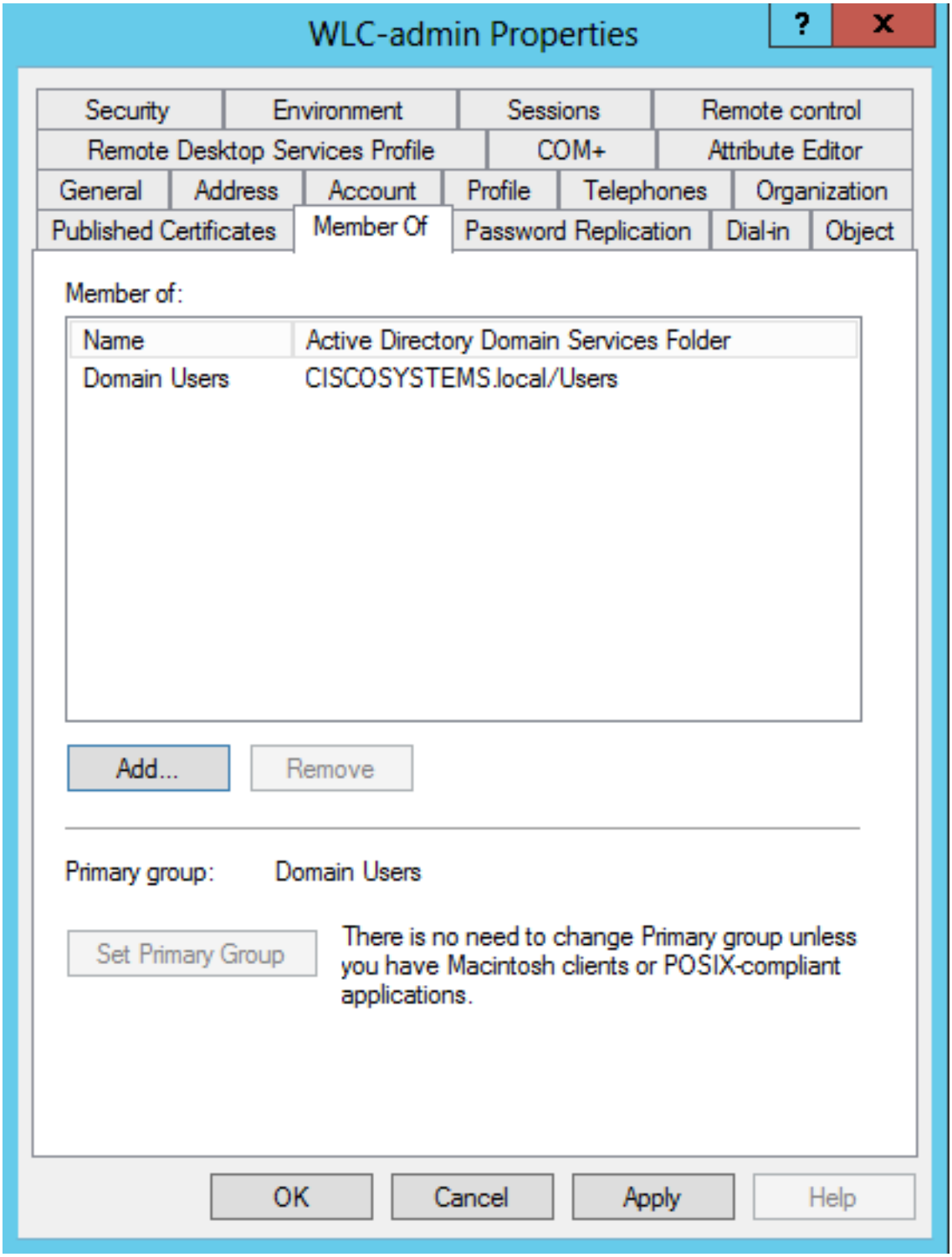
1. **Active Directory 사용자 및 컴퓨터를** 엽니다.

2. View **Advanced** Features(**고급 기능 보기)가** 선택되어 있는지 확인합니다.

3. 사용자 WLC-**admin으로** 이동하고 마우스 오른쪽 버튼을 클릭합니다. 이미지**에** 표시된 대로 컨텍스트 메뉴에서 속성을 선택합니다. 이 사용자는 WLC-admin이라는 이름으로 식별됩니다.

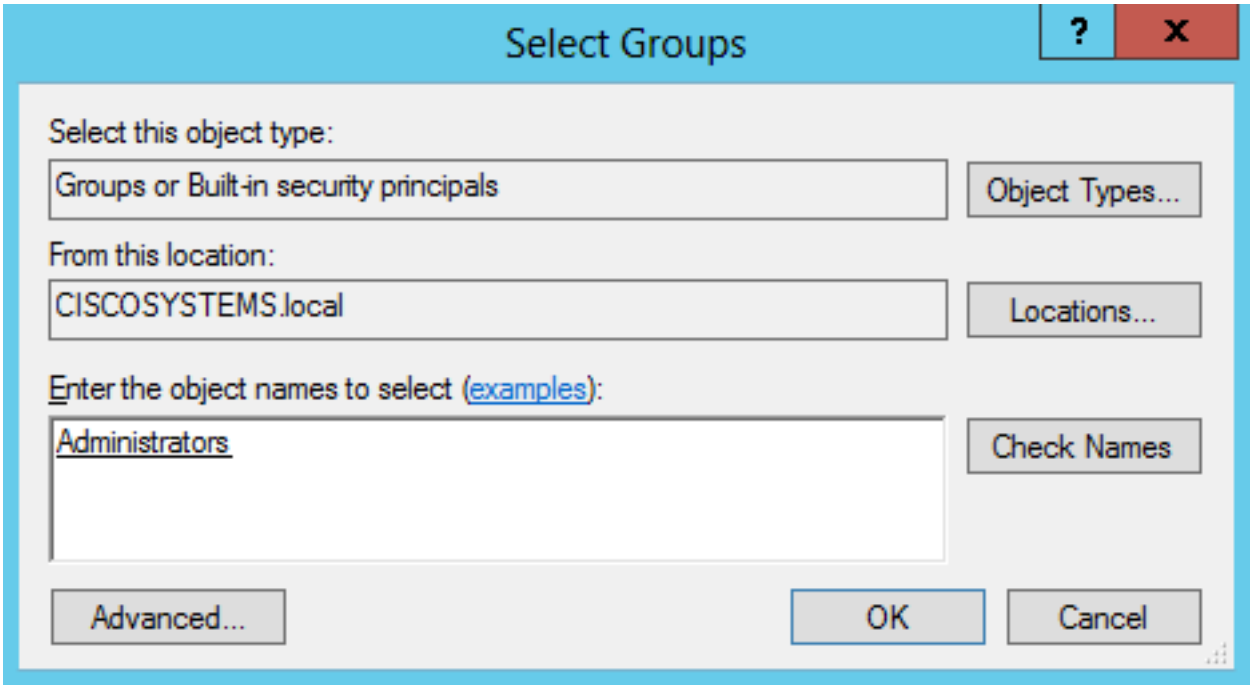


4. 이미지에 표시된 대로 **Member Of**(구성원) 탭을 클릭합니다.



::

5. **Add(추가)**를 클릭합니다. 열려 있는 대화 상자에서 Administrators를 **입력하고** 그림과 같이 **OK**(확인)를 클릭합니다.



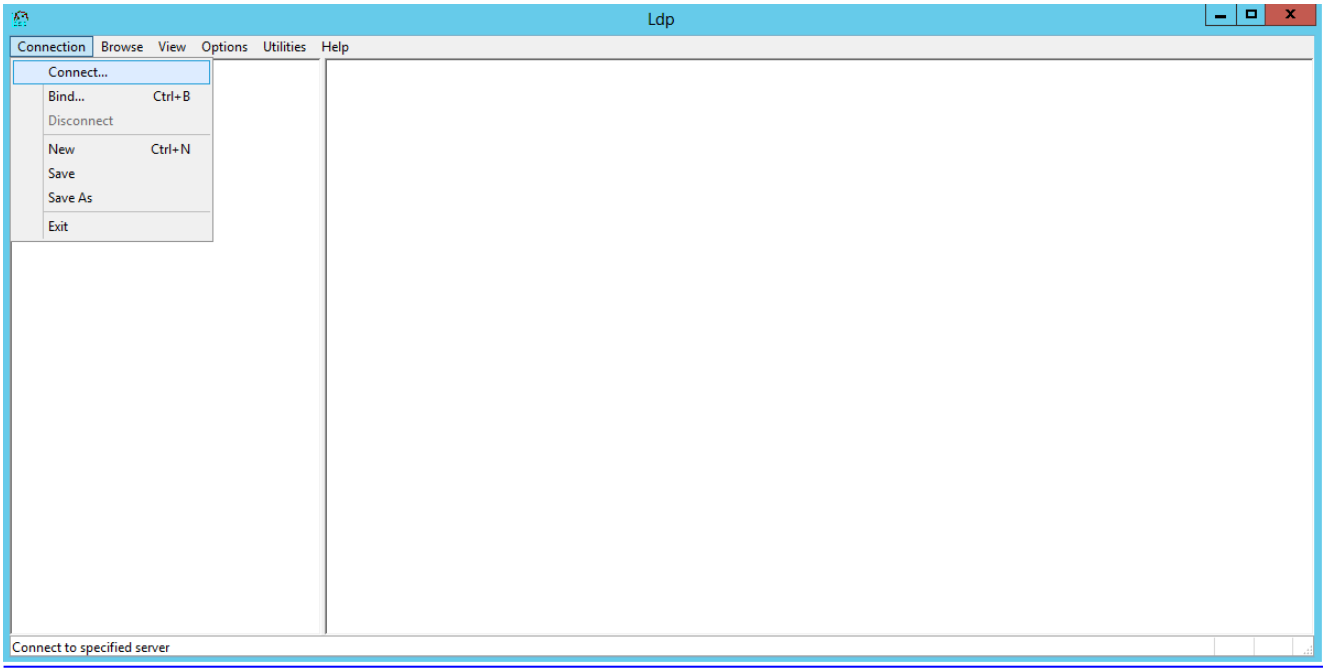
LDP를 사용하여 사용자 특성 식별

이 GUI 도구는 사용자가 Active Directory와 같은 LDAP 호환 디렉토리에 대해 연결, 바인딩, 검색, 수정, 추가 또는 삭제와 같은 작업을 수행할 수 있도록 하는 LDAP 클라이언트입니다. LDP는 보안 설명자 및 복제 메타데이터와 같은 메타데이터와 함께 Active Directory에 저장된 객체를 보는 데 사용됩니다.

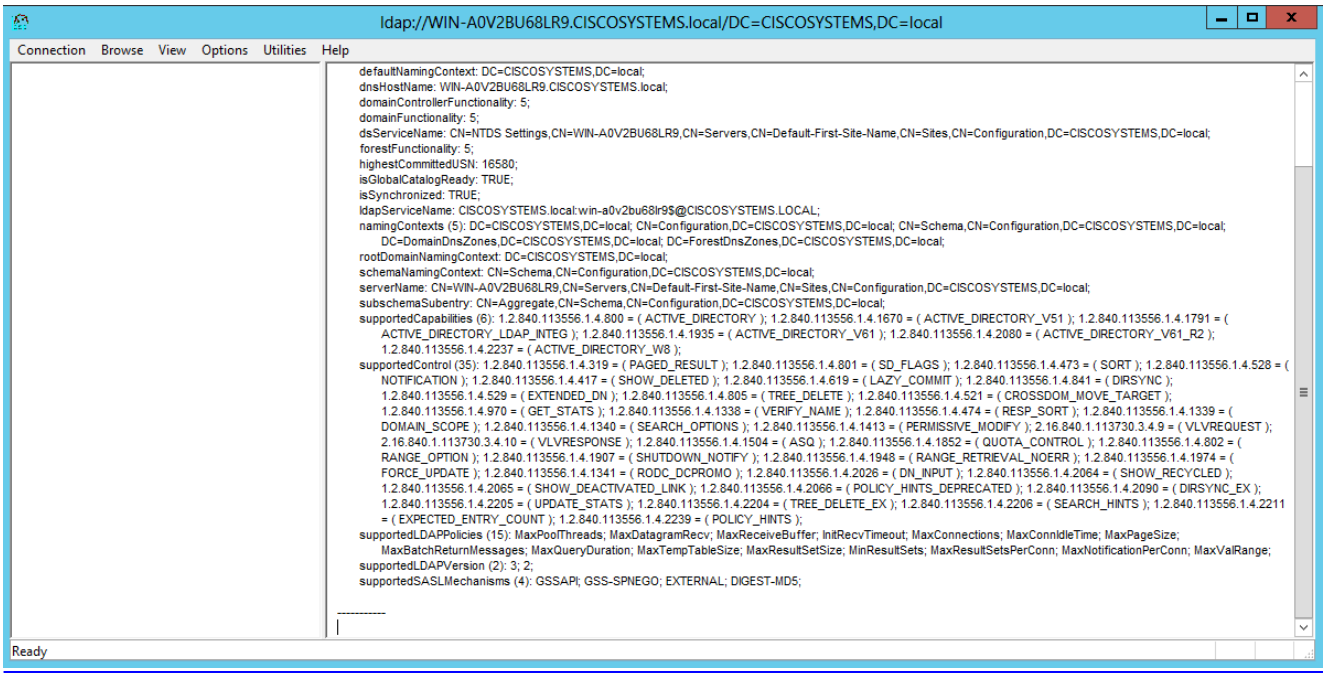
LDP GUI 도구는 제품 CD에서 Windows Server 2003 지원 도구를 설치할 때 포함됩니다. 이 섹션에서는 LDP 유틸리티를 사용하여 사용자 User1과 연관된 특정 속성을 식별하는 방법에 대해 설명합니다. 이러한 특성 중 일부는 WLC의 LDAP 서버 컨피그레이션 매개변수(예: User Attribute type 및 User Object type)를 채우는 데 사용됩니다.

1. Windows 2012 서버에서(동일한 LDAP 서버에서도) Windows PowerShell을 열고 LDP 브라우저에 액세스하기 위해 LDP를 입력합니다.

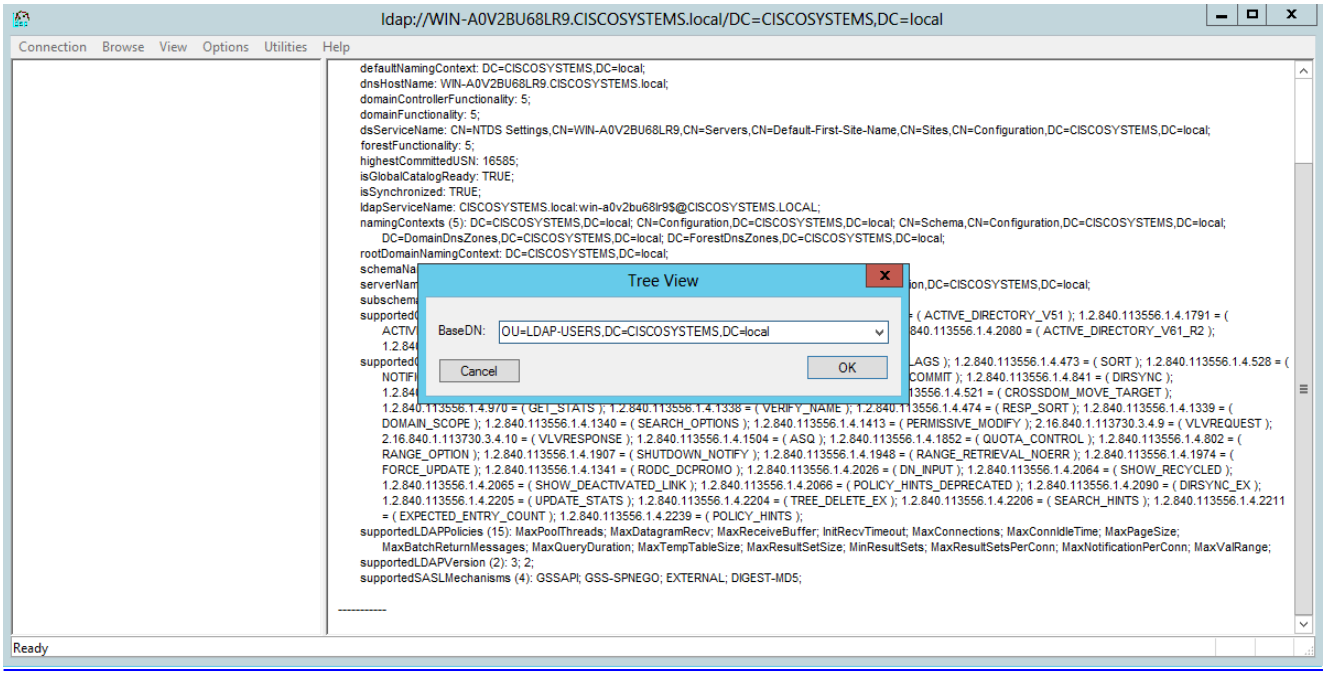
2. 이미지에 표시된 대로 LDAP 서버의 IP 주소를 입력하면 LDP 기본 창에서 **Connection(연결) > Connect(연결)**로 이동하여 LDAP 서버에 연결합니다.



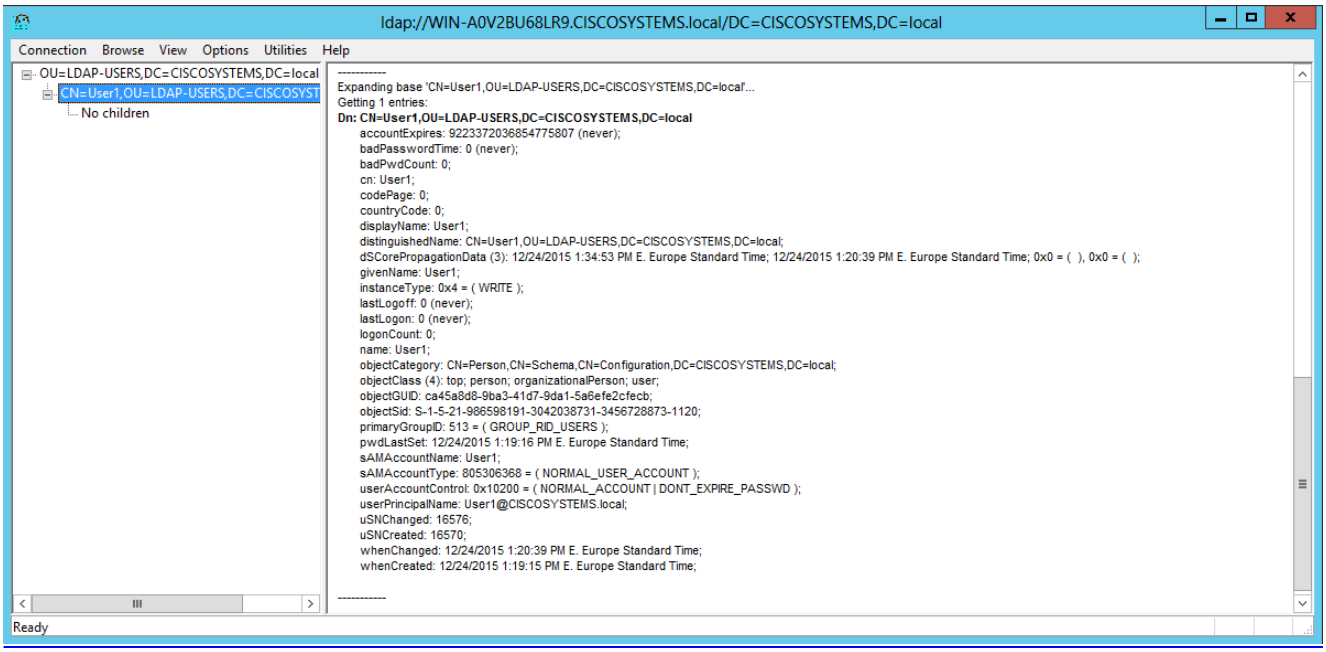
3. LDAP 서버에 연결되면 주 메뉴에서 **View**(보기)를 선택하고 **Tree(트리)**를 클릭합니다(이미지 참조).



4. 결과 트리 보기 창에서 사용자의 **BaseDN**을 입력합니다. 이 예에서 User1은 OU "LDAP-USERS" 아래의 CISCOSYSTEMS.local 도메인에 있습니다. 이미지에 표시된 대로 **OK**(확인)를 클릭합니다.



5. LDP 브라우저의 왼쪽에는 지정된 BaseDN(OU=LDAP-USERS, dc=CISCOSYSTEMS, dc=local) 아래에 나타나는 전체 트리가 표시됩니다. 트리를 확장하여 사용자 User1을 찾습니다. 이 사용자는 사용자의 이름을 나타내는 CN 값으로 식별될 수 있습니다. 이 예에서는 CN=User1입니다. **CN=User1**을 두 번 클릭합니다. 그림과 같이 LDP 브라우저의 오른쪽 창에 User1과 연결된 모든 특성이 표시됩니다.



6. LDAP 서버에 대해 WLC를 구성할 때 *User Attribute(사용자 특성)* 필드에 사용자 이름이 포함된 사용자 레코드의 특성 이름을 입력합니다. 이 LDP 출력에서 sAMAccountName이 사용자 이름 "User1"을 포함하는 하나의 특성임을 확인할 수 있으므로 WLC의 User Attribute 필드에 해당하는 sAMAccountName 특성을 입력합니다.

7. LDAP 서버에 대해 WLC를 구성할 때 *User Object Type(사용자 개체 유형)* 필드에 레코드를 사용자로 식별하는 LDAP objectType 특성의 값을 입력합니다. 사용자 레코드에는 objectType 특성에 대한 여러 값이 있는 경우가 많습니다. 그중 일부는 사용자에게 고유하고 일부는 다른 객체 유형과 공유됩니다. LDP 출력에서 CN=Person은 레코드를 사용자로 식별하는 한 값입니다. 따라서 WLC에서 **Person을** User Object Type 속성으로 지정합니다.다음 단계는 LDAP 서버에 대한 WLC를 구성하는 것입니다.

LDAP 서버에 대한 WLC 구성

이제 LDAP 서버가 구성되었으므로, 다음 단계는 LDAP 서버의 세부 사항으로 WLC를 구성하는 것입니다. WLC GUI에서 다음 단계를 완료합니다.

> **참고**:이 문서에서는 WLC가 기본 작동을 위해 구성되고 LAP가 WLC에 등록되어 있다고 가정합니다. LAP의 기본 작동을 위해 WLC를 설정하려는 새 사용자는 WLC(무선 LAN 컨트롤러)에 LAP(Lightweight AP) 등록을 참조하십시오.

1. WLC의 Security(보안) 페이지에서 왼쪽 작업창에서 **AAA > LDAP**를 선택하여 LDAP 서버 컨피그레이션 페이지로 이동합니다

.

LDAP 서버를 추가하려면 New(새로 만들기)를 **클릭합니다**. LDAP Servers(LDAP 서버) > New(새로 만들기) 페이지가 나타납니다.

2. LDAP Servers Edit(LDAP 서버 수정) 페이지에서 LDAP 서버의 IP 주소, Port Number(포트 번호), Enable Server status(서버 활성화 상태) 등 LDAP 서버의 세부 정보를 지정합니다.Server Index (Priority)(서버 인덱스(우선순위)) 드롭다운 상자에서 숫자를 선택하여 구성된 다른 LDAP 서버와 관련하여 이 서버의 우선순위를 지정합니다. 최대 17개의 서버를 구성할 수 있습니다. 컨트롤러가 첫 번째 서버에 도달할 수 없는 경우 목록의 두 번째 서버에 연결하는 등의 작업을 시도합니다.Server IP **Address 필드**에 LDAP 서버의 IP 주소를 입력합니다.Port Number(포트 번호) **필드**에 LDAP 서버의 **TCP 포트** 번호를 입력합니다. 유효한 범위는 1~65535이고 기본값은 389입니다.단순 바인딩의 경우 LDAP 서버 및 해당 비밀번호에 액세스하는 데 사용할 WLC 관리자 사용자의 위치인 바인드 사용자 이름에 대해 Authenticated를 사용했습니다User Base DN(사용자 기본 DN) 필드에 모든 **사용자**의 목록이 포함된 LDAP 서버에 있는 하위 트리의 DN**(고유 이름)**을 입력합니다. 예를 들어, ou=조직 단위, .ou=다음 조직 단위 및 o=corporation.com입니다. 사용자를 포함하는 트리가 기본 DN인 경우 o=corporation.com 또는 dc=corporation, dc=com을 입력합니다.이 예에서 사용자는 OU(Organizational Unit) LDAP-USERS 아래에 있으며, 이는 다시 lab.wireless 도메인의 일부로 생성됩니다.사용자 기본 DN은 사용자 정보(EAP-FAST 인증 방법에 따른 사용자 자격 증명)가 있는 전체 경로를 가리켜야 합니다. 이 예에서 사용자는 기본 DN OU=LDAP-USERS, DC=CISCOSYSTEMS, DC=local 아래에 있습니다.User Attribute(사용자 특성) 필드에 사용자 이름이 포함된 사용자 레코드의 특성 이름을 입력합니다.User Object Type 필드에 레코드를 사용자로 식별하는 LDAP objectType 특성의 값을 입력합니다. 사용자 레코드에는 objectType 특성에 대한 여러 값이 있는 경우가 많습니다. 그중 일부는 사용자에게 고유하고 일부는 다른 객체 유형과 공유됩니다Windows 2012 지원 도구의 일부로 제공되는 LDAP 브라우저 유틸리티를 사용하여 디렉토리 서버에서 이 두 필드의 값을 가져올 수 있습니다. 이 Microsoft LDAP 브라우저 도구를 LDP라고 합니다. 이 도구를 사용하면 이 특정 사용자의 User Base DN, User

Attribute 및 User Object Type 필드를 알 수 있습니다. LDP를 사용하여 이러한 사용자별 특성을 아는 방법에 대한 자세한 내용은 이 문서의 *사용자 특성 식별에 LDP* 사용 섹션에서 설명합니다.Server Timeout 필드에 재전송 간격(초)을 입력합니다. 유효한 범위는 2~30초이며 기본값은 2초입니다.Enable **Server Status(서버 상태** 활성화) 확인란을 선택하여 이 LDAP 서버를 활성화하거나 선택을 취소하여 비활성화합니다. 기본값은 disabled입니다.Apply(**적용**)를 클릭하여 변경 사항을 커밋합니다. 이 정보는 이미 구성된 예입니다

.

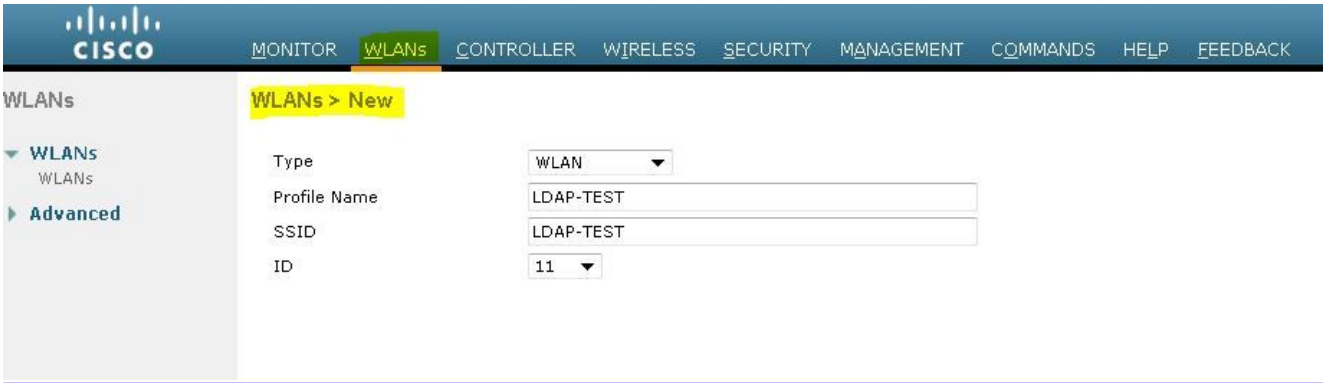
3. 이제 LDAP 서버에 대한 세부 정보가 WLC에 구성되었으므로 다음 단계는 웹 인증을 위해 WLAN을 구성하는 것입니다.

웹 인증을 위한 WLAN 구성

첫 번째 단계는 사용자를 위한 WLAN을 생성하는 것입니다. 다음 단계를 완료하십시오.

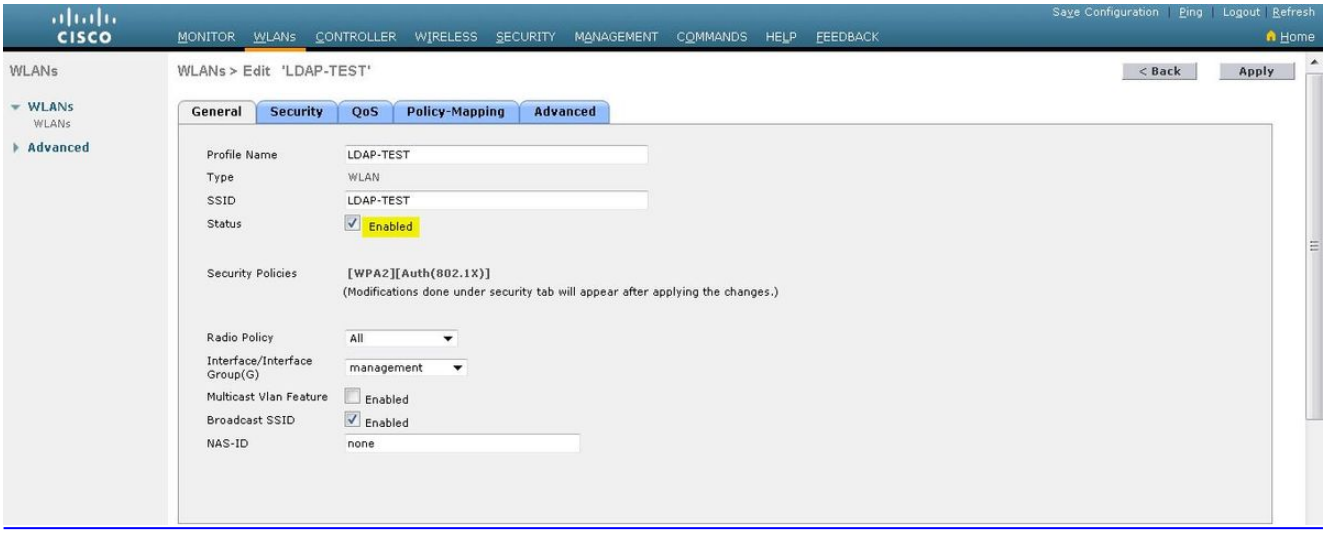
1. WLAN**을** 생성하려면 컨트롤러 GUI에서 WLANs를 클릭합니다.WLANs 창이 나타납니다. 이 창에는 컨트롤러에 구성된 WLAN이 나열됩니다.
2. 새 **WLAN**을 구성하려면 New(새로 만들기)를 클릭합니다.이 예에서 WLAN의 이름은 Web-Auth입니다

.



3. Apply를 **클릭합니다**.
4. WLAN > Edit(수정) 창에서 WLAN에 해당하는 매개변수를 정의합니다

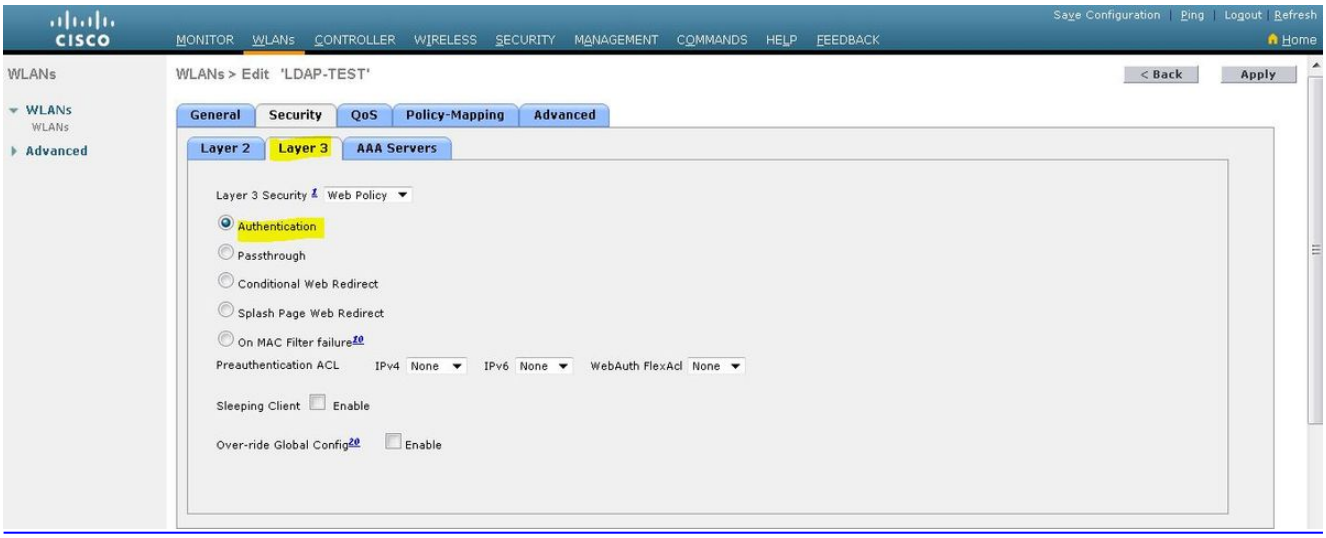
.



Status(상태) 확인란을 선택하여 WLAN을 활성화합니다.WLAN의 경우 Interface Name(인터페이스 이름) 필드에서 적절한 인터페이스를 선택합니다.이 예에서는 WLAN 웹 인증에 연결되는 관리 인터페이스를 매핑합니다.

5. **보안** 탭을 클릭합니다. Layer 3 Security(레이어 3 보안) 필드에서 **Web Policy(웹 정책)** 확인란을 선택하고 Authentication(**인증) 옵션을** 선택합니다

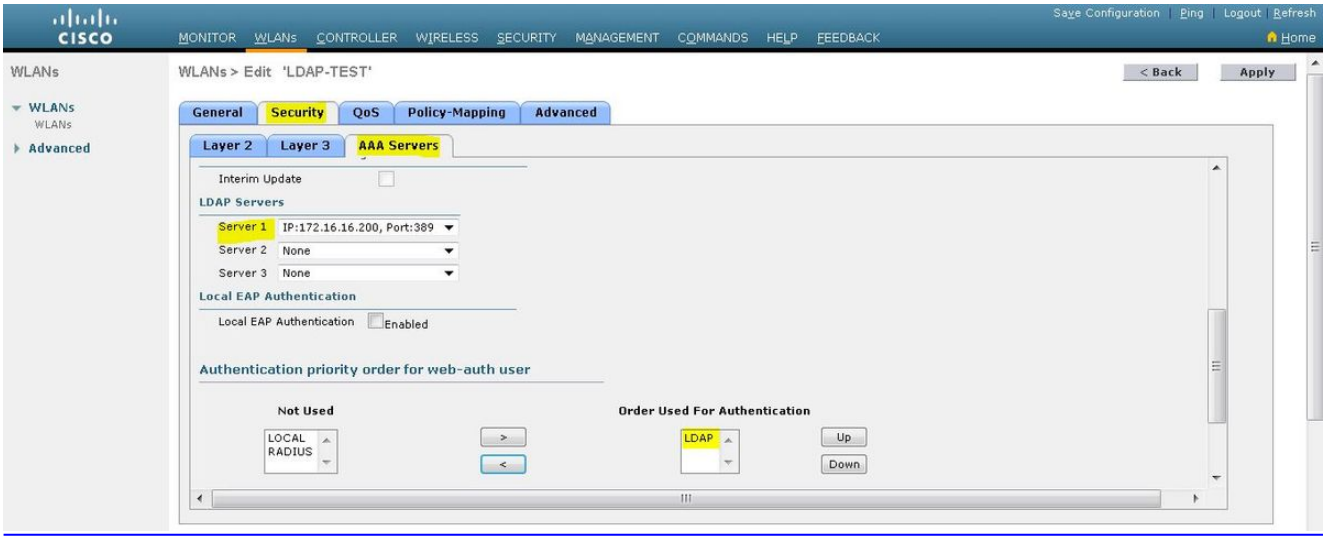
.



웹 인증이 무선 클라이언트를 인증하는 데 사용되므로 이 옵션이 선택됩니다. WLAN 웹 인증 **컨피그레이션**에 따라 활성화하려면 Override Global Config 확인란을 선택합니다. Web Auth type(웹 인증 유형) 드롭다운 메뉴에서 적절한 웹 인증 유형을 선택합니다. 이 예에서는 내부 웹 인증을 사용합니다.**참고**: 802.1x 인증에서는 웹 인증이 지원되지 않습니다. 즉, 웹 인증을 사용할 때 802.1x 또는 802.1x를 레이어 2 보안으로 사용하는 WPA/WPA2를 선택할 수 없습니다. 다른 모든 레이어 2 보안 매개변수에서는 웹 인증이 지원됩니다.

6. **AAA Servers(AAA 서버) 탭**을 클릭합니다. LDAP server(LDAP 서버) 풀다운 메뉴에서 구성된 LDAP 서버를 선택합니다. 로컬 데이터베이스 또는 RADIUS 서버를 사용하는 경우 *Authentication priority order for web-auth userfield(웹 인증 사용자 필드에 대한 인증 우선순위 순서) 아래에서 인증 우선순위를* 설정할 수 있습니다

.



7. Apply를 **클릭합니다**.**참고**: 이 예에서는 사용자 인증을 위한 Layer 2 Security 방법이 사용되지 않으므로 Layer 2 Security(레이어 2 보안) 필드에서 **None(없음**)을 선택합니다.

다음을 확인합니다.

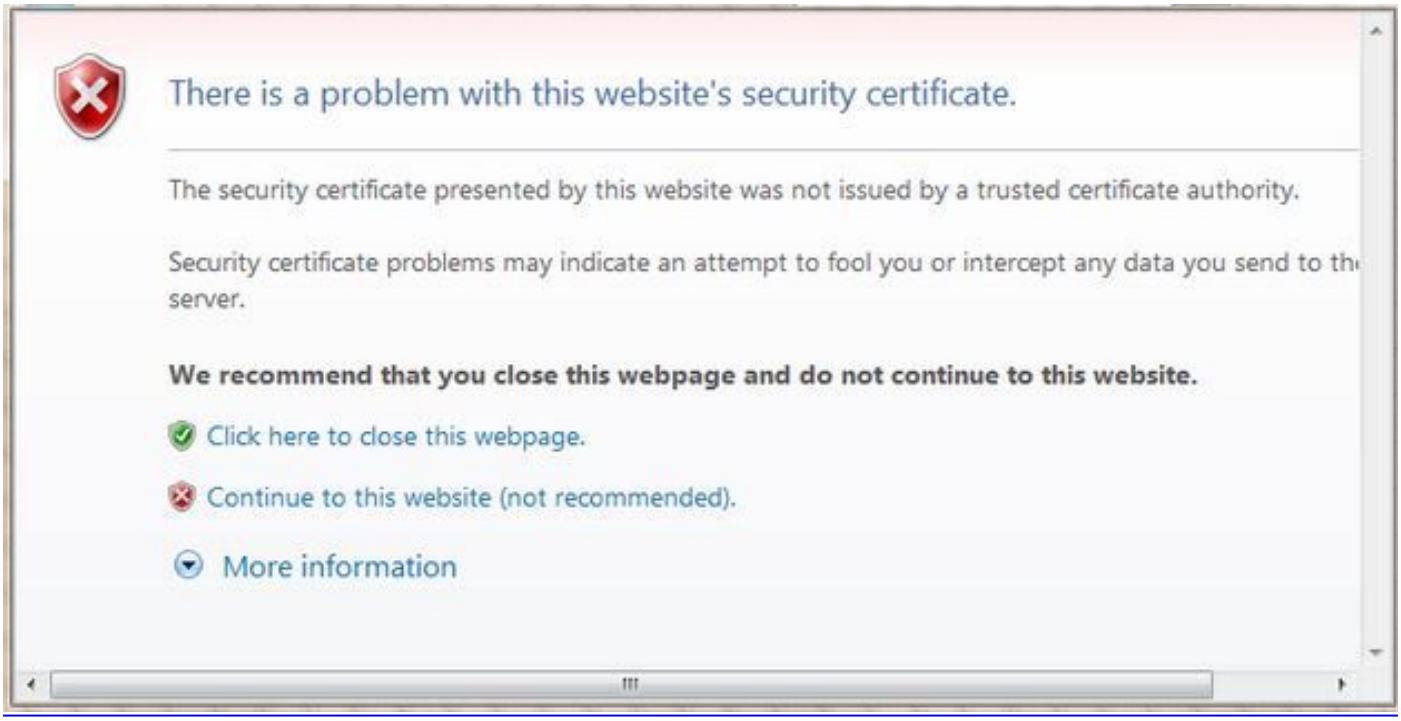
구성이 올바르게 작동하는지 확인하려면 이 섹션을 활용하십시오.

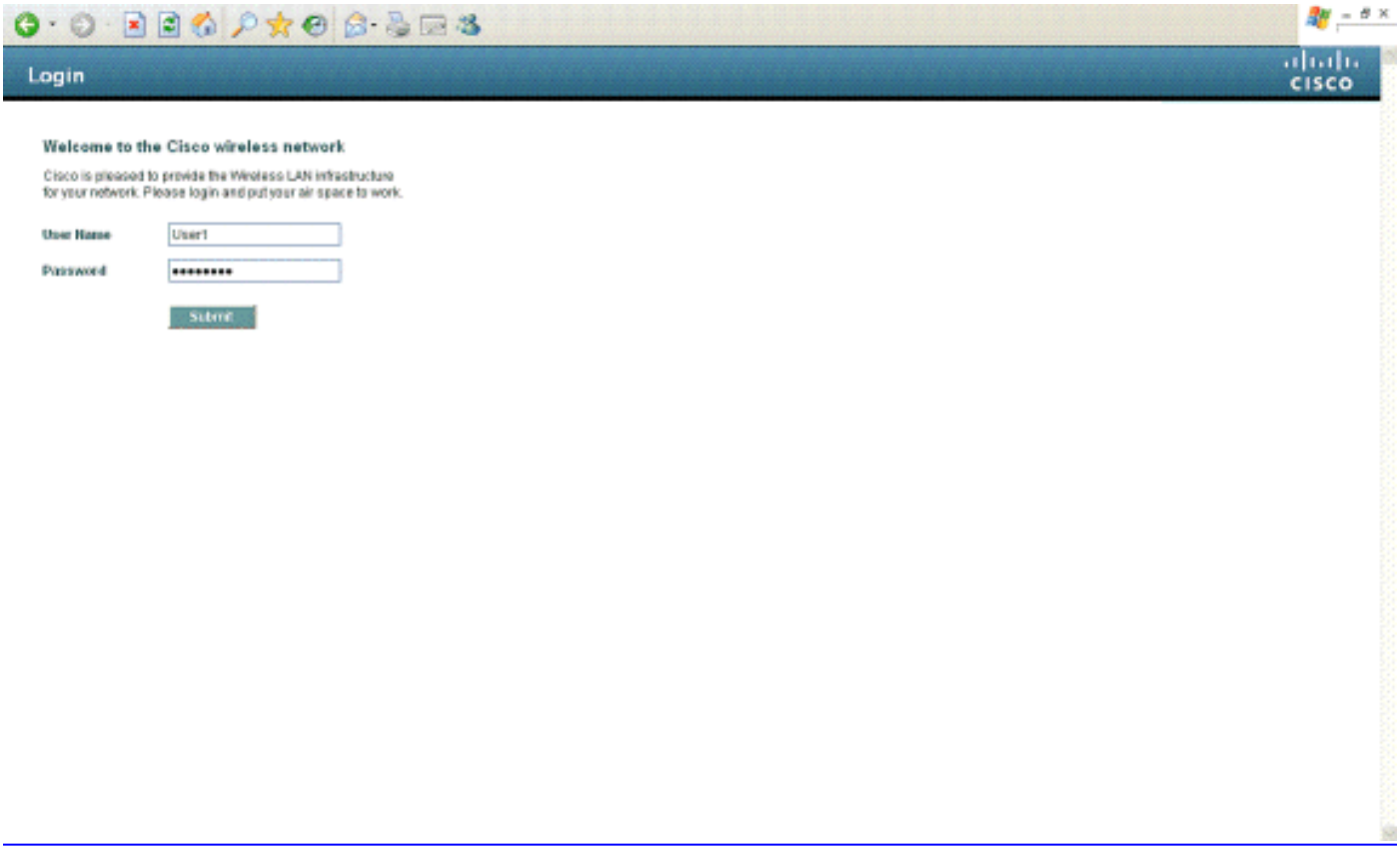
이 설정을 확인하려면 무선 클라이언트를 연결하고 컨피그레이션이 예상대로 작동하는지 확인하십시오.

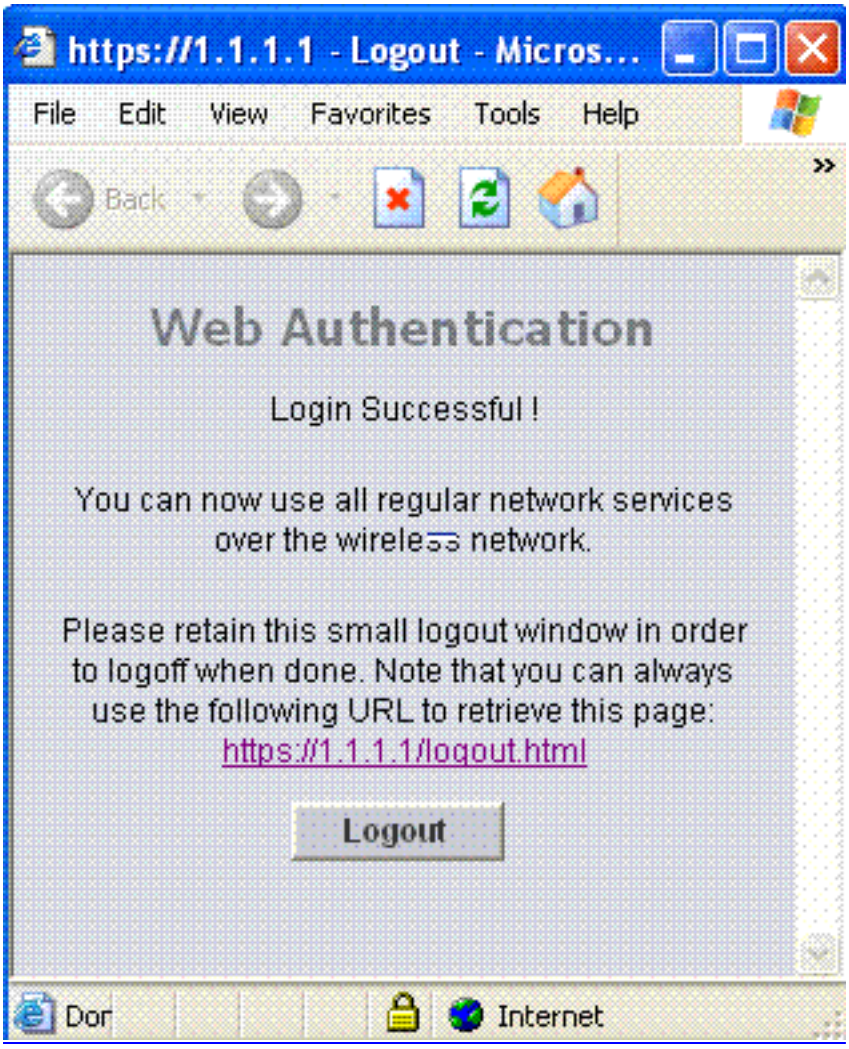
무선 클라이언트가 나타나고 사용자는 웹 브라우저에서 URL(예: www.yahoo.com)을 입력합니다. 사용자가 인증되지 않았으므로 WLC는 내부 웹 로그인 URL로 사용자를 리디렉션합니다.

사용자에게 사용자 자격 증명을 묻는 프롬프트가 표시됩니다. 사용자가 사용자 이름 및 비밀번호를 제출하면 로그인 페이지에서 사용자 자격 증명을 입력하고 제출 시 요청을 WLC 웹 서버의 action_URL 예(http://1.1.1.1/login.html)로 다시 전송합니다. 이는 고객 리디렉션 URL에 대한 입력 매개변수로 제공됩니다. 여기서 1.1.1.1은 스위치의 가상 인터페이스 주소입니다.

WLC는 LDAP 사용자 데이터베이스에 대해 사용자를 인증합니다. 인증에 성공하면 WLC 웹 서버는 사용자를 구성된 리디렉션 URL 또는 클라이언트가 시작된 URL(예: www.yahoo.com


There is a problem with this website's security certificate.
The security certificate presented by this website was not issued by a trusted certificate authority.
Security certificate problems may indicate an attempt to fool you or intercept any data you send to th
server.
We recommend that you close this webpage and do not continue to this website.
Click here to close this webpage.
Continue to this website (not recommended).
More information


Login
cisco
Welcome to the Cisco wireless network
Cisco is pleased to provide the Wireless LAN infrastructure
for your network. Please login and put your air space to work.
User Name
User1
Password
Submit



문제 해결

이 섹션에서는 설정 문제 해결에 사용할 수 있는 정보를 제공합니다.

컨피그레이션 트러블슈팅에 다음 명령을 사용합니다.

- **debug mac addr** <client-MAC-address xx:xx:xx:xx:xx>
- **debug aaa all enable**
- **디버그 pem 상태 활성화**
- **debug pem events enable**
- **debug dhcp message enable**
- **debug dhcp packet enable**

명령 debug mac addr cc**:fa:00:f7:32:35의 샘플 출력입니다.**

debug aaa ldap enable

```
(Cisco_Controller) >*pemReceiveTask: Dec 24 03:45:23.089: cc:fa:00:f7:32:35 Sent an XID frame
*apfMsConnTask_1: Dec 24 03:45:43.554: cc:fa:00:f7:32:35 Processing assoc-req
station:cc:fa:00:f7:32:35 AP:00:23:eb:e5:04:10-01 thread:18ec9330
*apfMsConnTask_1: Dec 24 03:45:43.554: cc:fa:00:f7:32:35 Association received from mobile on
BSSID 00:23:eb:e5:04:1f AP AP1142-1
*apfMsConnTask_1: Dec 24 03:45:43.554: cc:fa:00:f7:32:35 Global 200 Clients are allowed to AP
```

```
radio

*apfMsConnTask_1: Dec 24 03:45:43.554: cc:fa:00:f7:32:35 Max Client Trap Threshold: 0  cur: 1

*apfMsConnTask_1: Dec 24 03:45:43.554: cc:fa:00:f7:32:35 Rf profile 600 Clients are allowed to
AP wlan

*apfMsConnTask_1: Dec 24 03:45:43.554: cc:fa:00:f7:32:35 override for default ap group, marking
intgrp NULL
*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 Applying Interface policy on Mobile,
role Local. Ms NAC State 2 Quarantine Vlan 0 Access Vlan 16

*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 Re-applying interface policy for client

*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) Changing
IPv4 ACL 'none' (ACL ID 255) ===> 'none' (ACL ID 255) --- (caller apf_policy.c:2699)
*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) Changing
IPv6 ACL 'none' (ACL ID 255) ===> 'none' (ACL ID 255) --- (caller apf_policy.c:2720)
*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 apfApplyWlanPolicy: Apply WLAN Policy
over PMIPv6 Client Mobility Type, Tunnel User - 0
*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 In processSsidIE:6246 setting Central
switched to TRUE
*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 In processSsidIE:6249 apVapId = 1 and
Split Acl Id = 65535
*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 Applying site-specific Local Bridging
override for station cc:fa:00:f7:32:35 - vapId 1, site 'default-group', interface 'management'
*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 Applying Local Bridging Interface
Policy for station cc:fa:00:f7:32:35 - vlan 16, interface id 0, interface 'management'
*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 processSsidIE  statusCode is 0 and
status is 0
*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 processSsidIE  ssid_done_flag is 0
finish_flag is 0
*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 STA - rates (3): 24 164 48 0 0 0 0 0 0
0 0 0 0 0 0 0
*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 suppRates  statusCode is 0 and
gotSuppRatesElement is 1
*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 AID 2 in Assoc Req from flex AP
00:23:eb:e5:04:10 is same as in mscb cc:fa:00:f7:32:35
*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 apfMs1xStateDec
*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) Change
state to START (0) last state WEBAUTH_REQD (8)

*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 pemApfAddMobileStation2:
APF_MS_PEM_WAIT_L2_AUTH_COMPLETE = 0.
*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 172.16.16.122 START (0) Initializing
policy
*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 172.16.16.122 START (0) Change state to
AUTHCHECK (2) last state START (0)

*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 172.16.16.122 AUTHCHECK (2) Change
state to L2AUTHCOMPLETE (4) last state AUTHCHECK (2)

*pemReceiveTask: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 172.16.16.122 Removed NPU entry.
*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 Not Using WMM Compliance code qosCap 00
*apfMsConnTask_1: Dec 24 03:45:43.555: cc:fa:00:f7:32:35 172.16.16.122 L2AUTHCOMPLETE (4)
Plumbed mobile LWAPP rule on AP 00:23:eb:e5:04:10 vapId 1 apVapId 1 flex-acl-name:
*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 L2AUTHCOMPLETE (4) Change
state to WEBAUTH_REQD (8) last state L2AUTHCOMPLETE (4)

*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8)
pemApfAddMobileStation2 3802, Adding TMP rule
*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) Adding
Fast Path rule
 type = Airespace AP Client - ACL passthru
```

```
 on AP 00:23:eb:e5:04:10, slot 1, interface = 1, QOS = 0
 IPv4 ACL I
*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) Fast
Path rule (contd...) 802.1P = 0, DSCP = 0, TokenID = 15206, IntfId = 0  Local Bridging Vlan =
16, Local Bridging intf id = 0
*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) Fast
Path rule (contd...) AVC Ratelimit:  AppID = 0 ,AppAction = 4, AppToken = 15206  AverageRate =
0, BurstRate = 0

*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) Fast
Path rule (contd...) AVC Ratelimit:  AppID = 0 ,AppAction = 4, AppToken = 15206  AverageRate =
0, BurstRate = 0

*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) Fast
Path rule (contd...) AVC Ratelimit:  AppID = 0 ,AppAction = 4, AppToken = 15206  AverageRate =
0, BurstRate = 0

*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8)
Successfully plumbed mobile rule (IPv4 ACL ID 255, IPv6 ACL ID 255, L2 ACL ID 255)
*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8)
pemApfAddMobileStation2 3911, Adding TMP rule
*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8)
Replacing Fast Path rule
 type = Airespace AP Client - ACL passthru
 on AP 00:23:eb:e5:04:10, slot 1, interface = 1, QOS = 0
 IPv4 AC
*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) Fast
Path rule (contd...) 802.1P = 0, DSCP = 0, TokenID = 15206, IntfId = 0  Local Bridging Vlan =
16, Local Bridging intf id = 0
*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) Fast
Path rule (contd...) AVC Ratelimit:  AppID = 0 ,AppAction = 4, AppToken = 15206  AverageRate =
0, BurstRate = 0

*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) Fast
Path rule (contd...) AVC Ratelimit:  AppID = 0 ,AppAction = 4, AppToken = 15206  AverageRate =
0, BurstRate = 0

*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) Fast
Path rule (contd...) AVC Ratelimit:  AppID = 0 ,AppAction = 4, AppToken = 15206  AverageRate =
0, BurstRate = 0

*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8)
Successfully plumbed mobile rule (IPv4 ACL ID 255, IPv6 ACL ID 255, L2 ACL ID 255)
*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 apfPemAddUser2 (apf_policy.c:359)
Changing state for mobile cc:fa:00:f7:32:35 on AP 00:23:eb:e5:04:10 from Associated to
Associated

*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 apfPemAddUser2:session timeout
forstation cc:fa:00:f7:32:35 - Session Tout 1800, apfMsTimeOut '1800' and sessionTimerRunning
flag is  1
*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 Scheduling deletion of Mobile Station:
(callerId: 49) in 1800 seconds
*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 Func: apfPemAddUser2, Ms Timeout =
1800, Session Timeout = 1800

*apfMsConnTask_1: Dec 24 03:45:43.556: cc:fa:00:f7:32:35 Sending assoc-resp with status 0
station:cc:fa:00:f7:32:35 AP:00:23:eb:e5:04:10-01 on apVapId 1
*apfMsConnTask_1: Dec 24 03:45:43.557: cc:fa:00:f7:32:35 Sending Assoc Response to station on
BSSID 00:23:eb:e5:04:1f (status 0) ApVapId 1 Slot 1
*apfMsConnTask_1: Dec 24 03:45:43.557: cc:fa:00:f7:32:35 apfProcessAssocReq (apf_80211.c:10187)
Changing state for mobile cc:fa:00:f7:32:35 on AP 00:23:eb:e5:04:10 from Associated to
Associated

*pemReceiveTask: Dec 24 03:45:43.557: cc:fa:00:f7:32:35 172.16.16.122 Added NPU entry of type 2,
```

```
dtlFlags 0x0
*pemReceiveTask: Dec 24 03:45:43.557: cc:fa:00:f7:32:35 Sent an XID frame
*pemReceiveTask: Dec 24 03:45:43.557: cc:fa:00:f7:32:35 172.16.16.122 Added NPU entry of type 2,
dtlFlags 0x0
*pemReceiveTask: Dec 24 03:45:43.558: cc:fa:00:f7:32:35 Sent an XID frame
*DHCP Socket Task: Dec 24 03:45:43.708: cc:fa:00:f7:32:35 DHCP received op BOOTREQUEST (1) (len
322,vlan 16, port 1, encap 0xec03, xid 0x62743488)
*DHCP Socket Task: Dec 24 03:45:43.708: cc:fa:00:f7:32:35 DHCP (encap type 0xec03) mstype
0ff:ff:ff:ff:ff:ff
*DHCP Socket Task: Dec 24 03:45:43.708: cc:fa:00:f7:32:35 DHCP selecting relay 1 - control block
settings:
                        dhcpServer: 172.16.16.25, dhcpNetmask: 255.255.254.0,
                        dhcpGateway: 172.16.16.1, dhcpRelay: 172.16.16.25  VLAN: 16
*DHCP Socket Task: Dec 24 03:45:43.708: cc:fa:00:f7:32:35 DHCP mscbVapLocalAddr=172.16.16.25
mscbVapLocalNetMask= 255.255.254.0 mscbdhcpRelay=172.16.16.25
*DHCP Socket Task: Dec 24 03:45:43.708: cc:fa:00:f7:32:35 DHCP selected relay 1 - 172.16.16.25
(local address 172.16.16.25, gateway 172.16.16.25, VLAN 16, port 1)
*DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP selecting relay 2 - control block
settings:
                        dhcpServer: 172.16.16.25, dhcpNetmask: 255.255.254.0,
                        dhcpGateway: 172.16.16.1, dhcpRelay: 172.16.16.25  VLAN: 16
*DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP selected relay 2 - NONE
*DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP selecting relay 1 - control block
settings:
                        dhcpServer: 172.16.16.25, dhcpNetmask: 0.0.0.0,
                        dhcpGateway: 0.0.0.0, dhcpRelay: 172.16.16.25  VLAN: 16
*DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP mscbVapLocalAddr=172.16.16.25
mscbVapLocalNetMask= 255.255.254.0 mscbdhcpRelay=172.16.16.25
*DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP selected relay 1 - 172.16.16.25
(local address 172.16.16.25, gateway 172.16.16.25, VLAN 16, port 1)
*DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP transmitting DHCP DISCOVER (1)
*DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP   op: BOOTREQUEST, htype:
Ethernet, hlen: 6, hops: 1
*DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP   xid: 0x62743488 (1651782792),
secs: 0, flags: 0
*DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP   chaddr: cc:fa:00:f7:32:35
*DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP   ciaddr: 0.0.0.0,  yiaddr:
0.0.0.0
*DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP   siaddr: 0.0.0.0,  giaddr:
172.16.16.25
*DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP selecting relay 2 - control block
settings:
                        dhcpServer: 172.16.16.25, dhcpNetmask: 0.0.0.0,
                        dhcpGateway: 0.0.0.0, dhcpRelay: 172.16.16.25  VLAN: 16
*DHCP Socket Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP selected relay 2 - NONE
*DHCP Proxy Task: Dec 24 03:45:43.709: cc:fa:00:f7:32:35 DHCP received op BOOTREPLY (2) (len
572,vlan 0, port 0, encap 0x0, xid 0x62743488)
*DHCP Proxy Task: Dec 24 03:45:43.710: cc:fa:00:f7:32:35 DHCP sending REPLY to STA (len 418,
port 1, vlan 16)
*DHCP Proxy Task: Dec 24 03:45:43.710: cc:fa:00:f7:32:35 DHCP transmitting DHCP OFFER (2)
*DHCP Proxy Task: Dec 24 03:45:43.710: cc:fa:00:f7:32:35 DHCP   op: BOOTREPLY, htype: Ethernet,
hlen: 6, hops: 0
*DHCP Proxy Task: Dec 24 03:45:43.710: cc:fa:00:f7:32:35 DHCP   xid: 0x62743488 (1651782792),
secs: 0, flags: 0
*DHCP Proxy Task: Dec 24 03:45:43.710: cc:fa:00:f7:32:35 DHCP   chaddr: cc:fa:00:f7:32:35
*DHCP Proxy Task: Dec 24 03:45:43.710: cc:fa:00:f7:32:35 DHCP   ciaddr: 0.0.0.0,  yiaddr:
172.16.16.122
*DHCP Proxy Task: Dec 24 03:45:43.710: cc:fa:00:f7:32:35 DHCP   siaddr: 0.0.0.0,  giaddr:
0.0.0.0
*DHCP Proxy Task: Dec 24 03:45:43.710: cc:fa:00:f7:32:35 DHCP   server id: 1.1.1.1  rcvd server
id: 172.16.16.25
*DHCP Socket Task: Dec 24 03:45:43.714: cc:fa:00:f7:32:35 DHCP received op BOOTREQUEST (1) (len
334,vlan 16, port 1, encap 0xec03, xid 0x62743488)
*DHCP Socket Task: Dec 24 03:45:43.714: cc:fa:00:f7:32:35 DHCP (encap type 0xec03) mstype
```

```
0ff:ff:ff:ff:ff:ff
*DHCP Socket Task: Dec 24 03:45:43.714: cc:fa:00:f7:32:35 DHCP selecting relay 1 - control block
settings:
                        dhcpServer: 172.16.16.25, dhcpNetmask: 0.0.0.0,
                        dhcpGateway: 0.0.0.0, dhcpRelay: 172.16.16.25  VLAN: 16
*DHCP Socket Task: Dec 24 03:45:43.714: cc:fa:00:f7:32:35 DHCP mscbVapLocalAddr=172.16.16.25
mscbVapLocalNetMask= 255.255.254.0 mscbdhcpRelay=172.16.16.25
*DHCP Socket Task: Dec 24 03:45:43.714: cc:fa:00:f7:32:35 DHCP selected relay 1 - 172.16.16.25
(local address 172.16.16.25, gateway 172.16.16.25, VLAN 16, port 1)
*DHCP Socket Task: Dec 24 03:45:43.714: cc:fa:00:f7:32:35 DHCP transmitting DHCP REQUEST (3)
*DHCP Socket Task: Dec 24 03:45:43.714: cc:fa:00:f7:32:35 DHCP   op: BOOTREQUEST, htype:
Ethernet, hlen: 6, hops: 1
*DHCP Socket Task: Dec 24 03:45:43.714: cc:fa:00:f7:32:35 DHCP   xid: 0x62743488 (1651782792),
secs: 0, flags: 0
*DHCP Socket Task: Dec 24 03:45:43.714: cc:fa:00:f7:32:35 DHCP   chaddr: cc:fa:00:f7:32:35
*DHCP Socket Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP   ciaddr: 0.0.0.0,  yiaddr:
0.0.0.0
*DHCP Socket Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP   siaddr: 0.0.0.0,  giaddr:
172.16.16.25
*DHCP Socket Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP   requested ip: 172.16.16.122
*DHCP Socket Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP   server id: 172.16.16.25  rcvd
server id: 1.1.1.1
*DHCP Socket Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP selecting relay 2 - control block
settings:
                        dhcpServer: 172.16.16.25, dhcpNetmask: 0.0.0.0,
                        dhcpGateway: 0.0.0.0, dhcpRelay: 172.16.16.25  VLAN: 16
*DHCP Socket Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP selected relay 2 - NONE
*DHCP Proxy Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP received op BOOTREPLY (2) (len
572,vlan 0, port 0, encap 0x0, xid 0x62743488)
*DHCP Proxy Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP setting server from ACK
(mscb=0x40e64b88 ip=0xac10107a)(server 172.16.16.25, yiaddr 172.16.16.122)
*DHCP Proxy Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP sending REPLY to STA (len 418,
port 1, vlan 16)
*DHCP Proxy Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP transmitting DHCP ACK (5)
*DHCP Proxy Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP   op: BOOTREPLY, htype: Ethernet,
hlen: 6, hops: 0
*DHCP Proxy Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP   xid: 0x62743488 (1651782792),
secs: 0, flags: 0
*DHCP Proxy Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP   chaddr: cc:fa:00:f7:32:35
*DHCP Proxy Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP   ciaddr: 0.0.0.0,  yiaddr:
172.16.16.122
*DHCP Proxy Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP   siaddr: 0.0.0.0,  giaddr:
0.0.0.0
*DHCP Proxy Task: Dec 24 03:45:43.715: cc:fa:00:f7:32:35 DHCP   server id: 1.1.1.1  rcvd server
id: 172.16.16.25
*ewmwebWebauth1: Dec 24 03:46:01.222: cc:fa:00:f7:32:35 Username entry (User1) created for
mobile, length = 7
*ewmwebWebauth1: Dec 24 03:46:01.222: cc:fa:00:f7:32:35 Username entry (User1) created in mscb
for mobile, length = 7
*aaaQueueReader: Dec 24 03:46:01.222: AuthenticationRequest: 0x2b6bdc3c


*aaaQueueReader: Dec 24 03:46:01.222:   Callback.....................................0x12088c50

*aaaQueueReader: Dec 24 03:46:01.222:   protocolType.................................0x00000002

*aaaQueueReader: Dec 24 03:46:01.222:
proxyState.................................CC:FA:00:F7:32:35-00:00

*aaaQueueReader: Dec 24 03:46:01.222:   Packet contains 15 AVPs (not shown)

*LDAP DB Task 1: Dec 24 03:46:01.222: ldapTask [1] received msg 'REQUEST' (2) in state 'IDLE'
(1)
*LDAP DB Task 1: Dec 24 03:46:01.222: LDAP server 1 changed state to INIT
```

```
*LDAP DB Task 1: Dec 24 03:46:01.223: LDAP_OPT_REFERRALS = -1

*LDAP DB Task 1: Dec 24 03:46:01.223: ldapInitAndBind [1] called lcapi_init (rc = 0 - Success)
*LDAP DB Task 1: Dec 24 03:46:01.225: ldapInitAndBind [1] configured Method Authenticated
lcapi_bind (rc = 0 - Success)
*LDAP DB Task 1: Dec 24 03:46:01.225: LDAP server 1 changed state to CONNECTED
*LDAP DB Task 1: Dec 24 03:46:01.225: disabled LDAP_OPT_REFERRALS

*LDAP DB Task 1: Dec 24 03:46:01.225: LDAP_CLIENT: UID Search
(base=CN=Users,DC=CISCOSYSTEMS,DC=local, pattern=(&(objectclass=Person)(sAMAccountName=User1)))
*LDAP DB Task 1: Dec 24 03:46:01.226: LDAP_CLIENT: ldap_search_ext_s returns 0 -5
*LDAP DB Task 1: Dec 24 03:46:01.226: LDAP_CLIENT: Returned 2 msgs including 0 references
*LDAP DB Task 1: Dec 24 03:46:01.226: LDAP_CLIENT: Returned msg 1 type 0x64
*LDAP DB Task 1: Dec 24 03:46:01.226: LDAP_CLIENT: Received 1 attributes in search entry msg
*LDAP DB Task 1: Dec 24 03:46:01.226: LDAP_CLIENT: Returned msg 2 type 0x65
*LDAP DB Task 1: Dec 24 03:46:01.226: LDAP_CLIENT : No matched DN
*LDAP DB Task 1: Dec 24 03:46:01.226: LDAP_CLIENT : Check result error 0 rc 1013
*LDAP DB Task 1: Dec 24 03:46:01.226: LDAP_CLIENT: Received no referrals in search result msg
*LDAP DB Task 1: Dec 24 03:46:01.226: ldapAuthRequest [1] 172.16.16.200 - 389 called lcapi_query
base="CN=Users,DC=CISCOSYSTEMS,DC=local" type="Person" attr="sAMAccountName" user="User1" (rc =
0 - Success)
*LDAP DB Task 1: Dec 24 03:46:01.226: Attempting user bind with username
CN=User1,CN=Users,DC=CISCOSYSTEMS,DC=local
*LDAP DB Task 1: Dec 24 03:46:01.228: LDAP ATTR> dn = CN=User1,CN=Users,DC=CISCOSYSTEMS,DC=local
(size 45)
*LDAP DB Task 1: Dec 24 03:46:01.228: Handling LDAP response Success
*LDAP DB Task 1: Dec 24 03:46:01.228: Authenticated bind : Closing the binded session

*ewmwebWebauth1: Dec 24 03:46:01.228: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_REQD (8) Change
state to WEBAUTH_NOL3SEC (14) last state WEBAUTH_REQD (8)

*ewmwebWebauth1: Dec 24 03:46:01.228: cc:fa:00:f7:32:35 apfMsRunStateInc
*LDAP DB Task 1: Dec 24 03:46:01.228: ldapClose [1] called lcapi_close (rc = 0 - Success)
*ewmwebWebauth1: Dec 24 03:46:01.228: cc:fa:00:f7:32:35 172.16.16.122 WEBAUTH_NOL3SEC (14)
Change state to RUN (20) last state WEBAUTH_NOL3SEC (14)

*ewmwebWebauth1: Dec 24 03:46:01.228: cc:fa:00:f7:32:35 Stopping deletion of Mobile Station:
(callerId: 74)
*ewmwebWebauth1: Dec 24 03:46:01.228: cc:fa:00:f7:32:35 Setting Session Timeout to 1800 sec -
starting session timer for the mobile
*ewmwebWebauth1: Dec 24 03:46:01.228: cc:fa:00:f7:32:35 172.16.16.122 RUN (20) Reached
PLUMBFASTPATH: from line 6972
*ewmwebWebauth1: Dec 24 03:46:01.228: cc:fa:00:f7:32:35 172.16.16.122 RUN (20) Replacing Fast
Path rule
 type = Airespace AP Client
 on AP 00:23:eb:e5:04:10, slot 1, interface = 1, QOS = 0
 IPv4 ACL ID = 255, IPv6 ACL ID
*ewmwebWebauth1: Dec 24 03:46:01.228: cc:fa:00:f7:32:35 172.16.16.122 RUN (20) Fast Path rule
(contd...) 802.1P = 0, DSCP = 0, TokenID = 15206, IntfId = 0  Local Bridging Vlan = 16, Local
Bridging intf id = 0
*ewmwebWebauth1: Dec 24 03:46:01.228: cc:fa:00:f7:32:35 172.16.16.122 RUN (20) Fast Path rule
(contd...) AVC Ratelimit:  AppID = 0 ,AppAction = 4, AppToken = 15206  AverageRate = 0,
BurstRate = 0

*ewmwebWebauth1: Dec 24 03:46:01.228: cc:fa:00:f7:32:35 172.16.16.122 RUN (20) Fast Path rule
(contd...) AVC Ratelimit:  AppID = 0 ,AppAction = 4, AppToken = 15206  AverageRate = 0,
BurstRate = 0

*ewmwebWebauth1: Dec 24 03:46:01.228: cc:fa:00:f7:32:35 172.16.16.122 RUN (20) Fast Path rule
(contd...) AVC Ratelimit:  AppID = 0 ,AppAction = 4, AppToken = 15206  AverageRate = 0,
BurstRate = 0

*ewmwebWebauth1: Dec 24 03:46:01.229: cc:fa:00:f7:32:35 172.16.16.122 RUN (20) Successfully
plumbed mobile rule (IPv4 ACL ID 255, IPv6 ACL ID 255, L2 ACL ID 255)
```

```
*pemReceiveTask: Dec 24 03:46:01.229: cc:fa:00:f7:32:35 172.16.16.122 Added NPU entry of type 1,
dtlFlags 0x0


(Cisco_Controller) >show client detail cc:fa:00:f7:32:35
Client MAC Address.............................. cc:fa:00:f7:32:35
Client Username ................................ User1
AP MAC Address.................................. 00:23:eb:e5:04:10
AP Name......................................... AP1142-1
AP radio slot Id................................ 1
Client State.................................... Associated
Client User Group............................... User1
Client NAC OOB State............................ Access
Wireless LAN Id................................. 1
Wireless LAN Network Name (SSID)................ LDAP-TEST
Wireless LAN Profile Name....................... LDAP-TEST
Hotspot (802.11u)............................... Not Supported
BSSID........................................... 00:23:eb:e5:04:1f
Connected For .................................. 37 secs
Channel......................................... 36
IP Address...................................... 172.16.16.122
Gateway Address................................. 172.16.16.1
Netmask......................................... 255.255.254.0
Association Id.................................. 2
Authentication Algorithm........................ Open System
Reason Code..................................... 1
Status Code..................................... 0

--More or (q)uit current module or <ctrl-z> to abort
Session Timeout................................. 1800
Client CCX version.............................. No CCX support
QoS Level....................................... Silver
Avg data Rate................................... 0
Burst data Rate................................. 0
Avg Real time data Rate......................... 0
Burst Real Time data Rate....................... 0
802.1P Priority Tag............................. disabled
CTS Security Group Tag.......................... Not Applicable
KTS CAC Capability.............................. No
Qos Map Capability.............................. No
WMM Support..................................... Enabled
 APSD ACs.....................................  BK  BE  VI  VO
Current Rate.................................... m7
Supported Rates................................. 12.0,18.0,24.0
Mobility State.................................. Local
Mobility Move Count............................. 0
Security Policy Completed....................... Yes
Policy Manager State............................ RUN
Audit Session ID................................ ac10101900000005567b69f8
AAA Role Type................................... none
Local Policy Applied............................ none
IPv4 ACL Name................................... none

--More or (q)uit current module or <ctrl-z> to abort
FlexConnect ACL Applied Status.................. Unavailable
IPv4 ACL Applied Status......................... Unavailable
IPv6 ACL Name................................... none
IPv6 ACL Applied Status......................... Unavailable
Layer2 ACL Name................................. none
Layer2 ACL Applied Status....................... Unavailable
Client Type..................................... SimpleIP
mDNS Status..................................... Enabled
mDNS Profile Name............................... default-mdns-profile
No. of mDNS Services Advertised................. 0
```

```
Policy Type..................................... N/A
Encryption Cipher............................... None
Protected Management Frame ..................... No
Management Frame Protection..................... No
EAP Type........................................ Unknown
FlexConnect Data Switching...................... Central
FlexConnect Dhcp Status......................... Central
FlexConnect Vlan Based Central Switching........ No
FlexConnect Authentication...................... Central
FlexConnect Central Association................. No
Interface....................................... management
VLAN............................................ 16
Quarantine VLAN................................. 0

--More or (q)uit current module or <ctrl-z> to abort
Access VLAN..................................... 16
Local Bridging VLAN............................. 16
Client Capabilities:
     CF Pollable................................ Not implemented
     CF Poll Request............................ Not implemented
     Short Preamble............................. Not implemented
     PBCC....................................... Not implemented
     Channel Agility............................ Not implemented
     Listen Interval............................ 10
     Fast BSS Transition........................ Not implemented
     11v BSS Transition......................... Not implemented
Client Wifi Direct Capabilities:
     WFD capable................................ No
     Manged WFD capable......................... No
     Cross Connection Capable................... No
     Support Concurrent Operation............... No
Fast BSS Transition Details:
Client Statistics:
     Number of Bytes Received................... 16853
     Number of Bytes Sent....................... 31839
     Total Number of Bytes Sent................. 31839
     Total Number of Bytes Recv................. 16853
     Number of Bytes Sent (last 90s)............ 31839

--More or (q)uit current module or <ctrl-z> to abort
     Number of Bytes Recv (last 90s)............ 16853
     Number of Packets Received................. 146
     Number of Packets Sent..................... 92
     Number of Interim-Update Sent.............. 0
     Number of EAP Id Request Msg Timeouts...... 0
     Number of EAP Id Request Msg Failures...... 0
     Number of EAP Request Msg Timeouts......... 0
     Number of EAP Request Msg Failures......... 0
     Number of EAP Key Msg Timeouts............. 0
     Number of EAP Key Msg Failures............. 0
     Number of Data Retries..................... 2
     Number of RTS Retries...................... 0
     Number of Duplicate Received Packets....... 0
     Number of Decrypt Failed Packets........... 0
     Number of Mic Failured Packets............. 0
     Number of Mic Missing Packets.............. 0
     Number of RA Packets Dropped............... 0
     Number of Policy Errors.................... 0
     Radio Signal Strength Indicator............ -48 dBm
     Signal to Noise Ratio...................... 41 dB
Client Rate Limiting Statistics:
     Number of Data Packets Received............ 0
     Number of Data Rx Packets Dropped.......... 0
```

```
--More or (q)uit current module or <ctrl-z> to abort
     Number of Data Bytes Received.............. 0
     Number of Data Rx Bytes Dropped............ 0
     Number of Realtime Packets Received........ 0
     Number of Realtime Rx Packets Dropped...... 0
     Number of Realtime Bytes Received.......... 0
     Number of Realtime Rx Bytes Dropped........ 0
     Number of Data Packets Sent................ 0
     Number of Data Tx Packets Dropped.......... 0
     Number of Data Bytes Sent.................. 0
     Number of Data Tx Bytes Dropped............ 0
     Number of Realtime Packets Sent............ 0
     Number of Realtime Tx Packets Dropped...... 0
     Number of Realtime Bytes Sent.............. 0
     Number of Realtime Tx Bytes Dropped........ 0
Nearby AP Statistics:
     AP1142-1(slot 0)
       antenna0: 25 secs ago..................... -37 dBm
       antenna1: 25 secs ago..................... -37 dBm
     AP1142-1(slot 1)
       antenna0: 25 secs ago..................... -44 dBm
       antenna1: 25 secs ago..................... -57 dBm
DNS Server details:
     DNS server IP ............................. 0.0.0.0

--More or (q)uit current module or <ctrl-z> to abort
     DNS server IP ............................. 0.0.0.0
Assisted Roaming Prediction List details:


Client Dhcp Required:     False
```

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.