RSA SecurID Ready with Wireless LAN Controller 및 Cisco Secure ACS 구성 예

목차

소개

이 문서에서는 RSA SecurID 인증 WLAN 환경에서 사용할 Cisco LWAPP(Lightweight Access Point Protocol) 지원 AP 및 WLC(Wireless LAN Controller)와 Cisco ACS(Secure Access Control Server)를 설정하고 구성하는 방법에 대해 설명합니다.RSA SecurID 관련 구현 가이드는 www.rsasecured.com에서 확인할 수 있습니다.

사전 요구 사항

요구 사항

이 구성을 시도하기 전에 다음 요구 사항을 충족해야 합니다.

- WLC에 대한 지식 및 WLC 기본 매개변수를 구성하는 방법.
- ADU(Aironet Desktop Utility)를 사용하여 Cisco Wireless Client의 프로필을 구성하는 방법에 대한 지식
- Cisco Secure ACS에 대한 기능 지식이 있어야 합니다.
- LWAPP에 대한 기본적인 지식을 갖추십시오.
- Microsoft Windows AD(Active Directory) 서비스는 물론 도메인 컨트롤러 및 DNS 개념에 대한

기본적인 이해가 있어야 합니다.**참고:** 이 구성을 시도하기 전에 ACS와 RSA Authentication Manager 서버가 동일한 도메인에 있고 해당 시스템 클럭이 정확히 동기화되었는지 확인하십시오.Microsoft Windows AD 서비스를 사용하는 경우 Microsoft 설명서를 참조하여 동일한 도메인에서 ACS 및 RSA Manager 서버를 구성합니다.관련 정보는 Active Directory 및 Windows 사용자 데이터베이스 구성을 참조하십시오.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- RSA Authentication Manager 6.1
- Microsoft Windows용 RSA Authentication Agent 6.1
- Cisco Secure ACS 4.0(1) 빌드 27**참고:** 포함된 RADIUS 서버는 Cisco ACS 대신 사용할 수 있습니다.서버를 구성하는 방법은 RSA 인증 관리자에 포함된 RADIUS 설명서를 참조하십시오.
- Cisco WLC 및 Lightweight Access Point for Release 4.0(버전 4.0.155.0)

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.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 규칙을 참조하십시오.

배경 정보

RSA SecurID 시스템은 2단계 사용자 인증 솔루션입니다.RSA Authentication Manager 및 RSA Authentication Agent와 함께 사용되는 RSA SecurID 인증자는 사용자가 2단계 인증 메커니즘을 사용하여 자신을 식별해야 합니다.

하나는 RSA SecurID 코드입니다. RSA SecureID 인증 디바이스에서 60초마다 생성되는 난수입니다.다른 하나는 PIN(개인 식별 번호)입니다.

RSA SecurID 인증자는 비밀번호 입력과 같이 사용하기 쉽습니다.각 최종 사용자에게 일회용 코드를 생성하는 RSA SecurID 인증자가 할당됩니다.로그온하면 이 번호와 비밀 PIN을 입력하여 성공적으로 인증됩니다.RSA SecurID 하드웨어 토큰은 일반적으로 수신 시 완벽하게 작동하도록 사전 프로그래밍됩니다.

이 플래시 데모에서는 RSA secureID 인증자 디바이스를 사용하는 방법에 대해 설명합니다.RSA 데모.

Cisco WLC와 Cisco Secure ACS 서버는 RSA SecurID Ready 프로그램을 통해 즉시 RSA SecurID 인증을 지원합니다.RSA 인증 에이전트 소프트웨어는 로컬 또는 원격 사용자(또는 사용자 그룹)로부터 액세스 요청을 인터셉트하고 인증을 위해 RSA 인증 관리자 프로그램으로 전달합니다.

RSA Authentication Manager 소프트웨어는 RSA SecurID 솔루션의 관리 구성 요소입니다.인증 요청을 확인하고 엔터프라이즈 네트워크에 대한 인증 정책을 중앙에서 관리하는 데 사용됩니다.RSA SecurID 인증자 및 RSA Authentication Agent 소프트웨어와 함께 작동합니다.

이 문서에서는 에이전트 소프트웨어를 설치하여 Cisco ACS 서버를 RSA 인증 에이전트로 사용합니다.WLC는 NAS(Network Access Server)(AAA 클라이언트)로, ACS에 클라이언트 인증을 전달합

니다.이 문서에서는 PEAP(Protected Extensible Authentication Protocol) 클라이언트 인증을 사용하여 개념과 설정을 보여 줍니다.

PEAP 인증에 대한 자세한 내용은 Cisco Protected Extensible Authentication Protocol을 참조하십시오.

구성

이 섹션에는 이 문서에서 설명하는 기능을 구성하기 위한 정보가 표시됩니다.

이 문서에서는 다음 구성을 사용합니다.

- 에이전트 호스트 구성
- 인증 에이전트 구성

에이전트 호스트 구성

Cisco Secure ACS를 RADIUS 서버로 사용

Cisco Secure ACS와 RSA Authentication Manager/RSA SecurID Appliance 간의 통신을 용이하게 하려면 에이전트 호스트 레코드를 RSA Authentication Manager 데이터베이스에 추가해야 합니다.에이전트 호스트 레코드는 데이터베이스 내의 Cisco Secure ACS를 식별하고 통신 및 암호화에 대한 정보를 포함합니다.

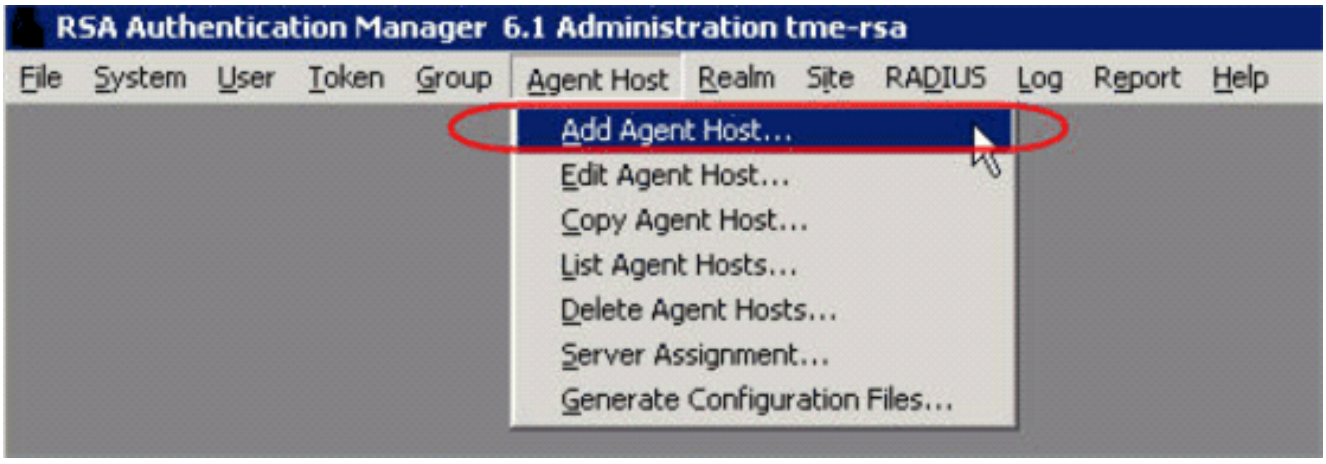
에이전트 호스트 레코드를 만들려면 다음 정보가 필요합니다.

- Cisco ACS 서버의 호스트 이름
- Cisco ACS 서버의 모든 네트워크 인터페이스에 대한 IP 주소

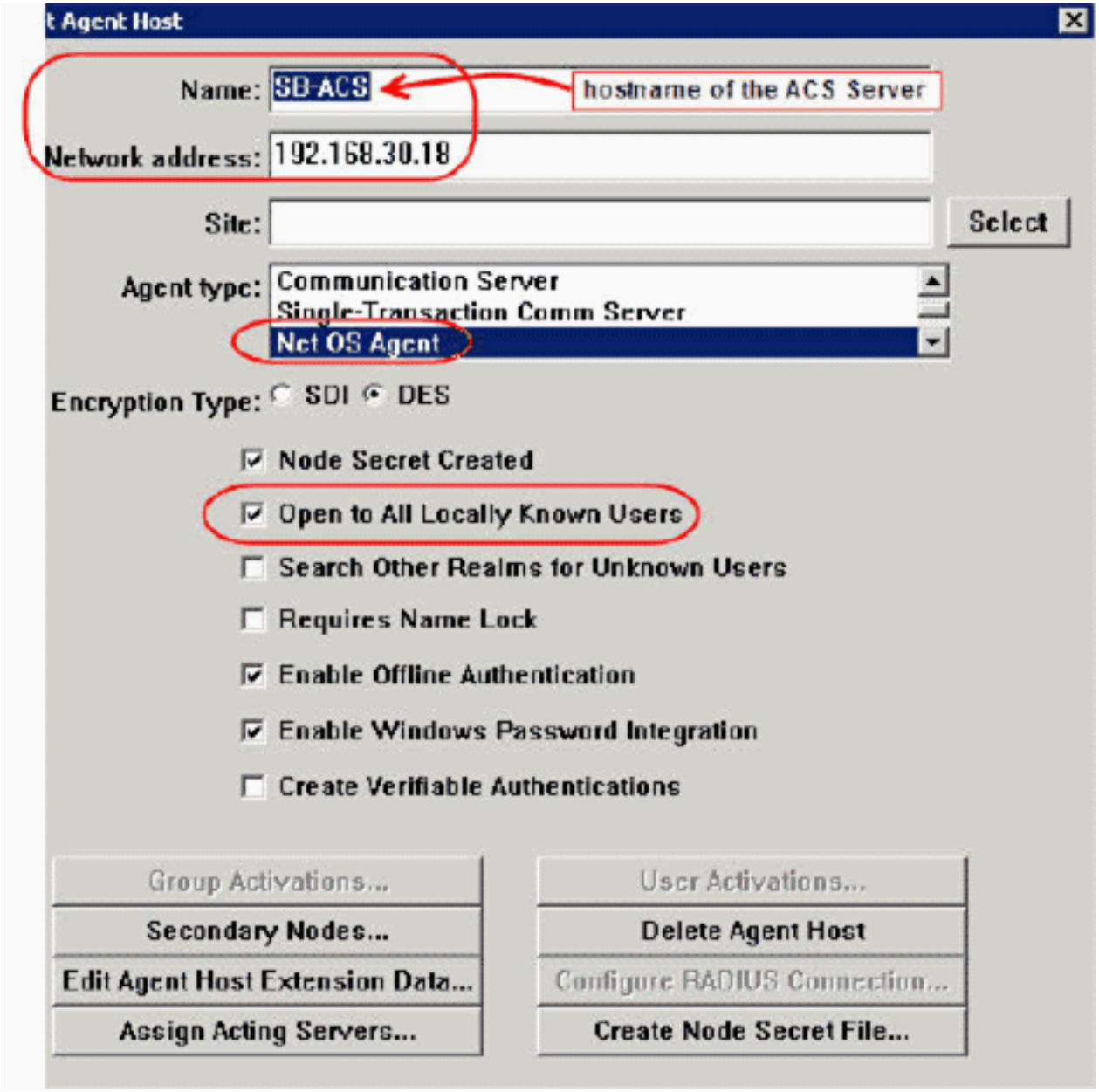
다음 단계를 완료하십시오.

1. RSA 인증 관리자 호스트 모드 애플리케이션을 엽니다.
2. Agent **Host > Add Agent Host를 선택합니다**

.



이 창이 표시됩니다



3. Cisco ACS 서버 이름 및 네트워크 주소에 대한 적절한 정보를 입력합니다.Agent 유형에 대해 NetOS를 선택하고 Open to All Locally Known Users(로컬로 알려진 모든 사용자에게 열기) 확인란**을 선택합니다**.
4. **확인**을 **클릭합니다**.

RSA Authentication Manager 6.1 RADIUS 서버 사용

Cisco WLC와 RSA Authentication Manager 간의 원활한 통신을 위해 에이전트 호스트 레코드를 RSA Authentication Manager 데이터베이스 및 RADIUS 서버 데이터베이스에 추가해야 합니다.에이전트 호스트 레코드는 데이터베이스 내의 Cisco WLC를 식별하고 통신 및 암호화에 대한 정보를 포함합니다.

에이전트 호스트 레코드를 만들려면 다음 정보가 필요합니다.

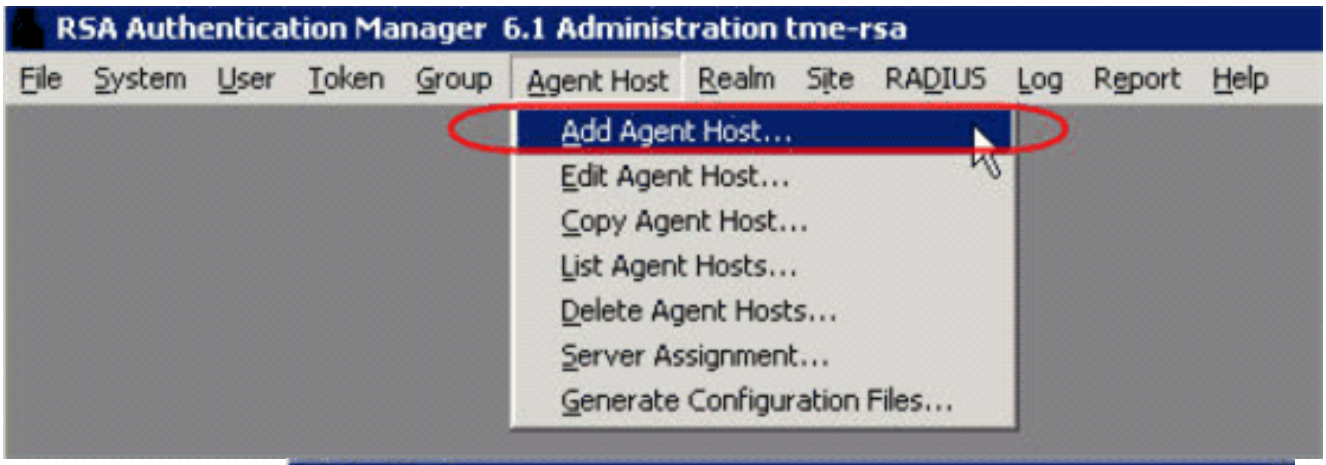
- WLC의 호스트 이름
- WLC의 관리 IP 주소
- RADIUS 암호 - Cisco WLC의 RADIUS 암호와 일치해야 함

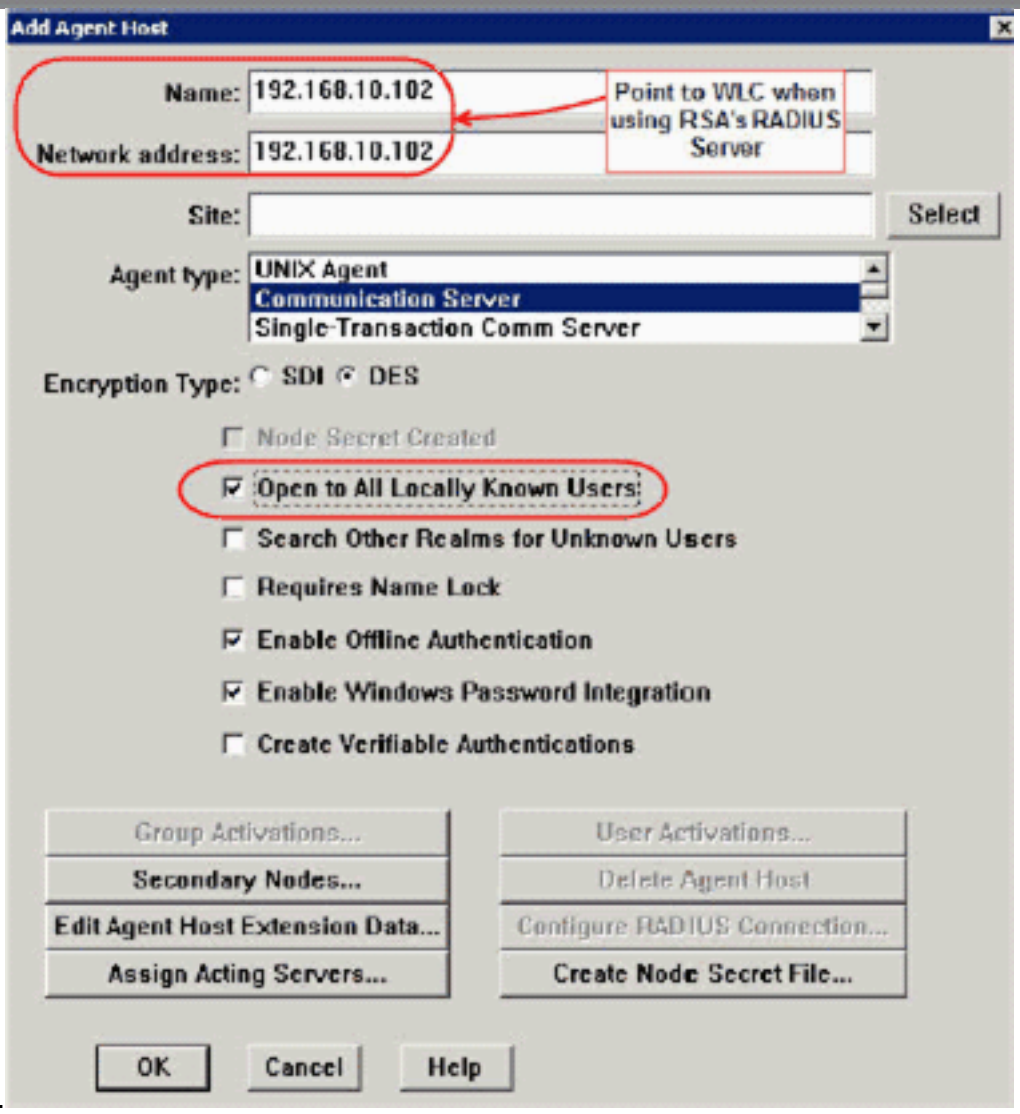
에이전트 호스트 레코드를 추가할 때 WLC의 역할은 통신 서버로 구성됩니다.이 설정은 RSA Authentication Manager에서 WLC와의 통신 방식을 결정하는 데 사용됩니다.

참고: RSA Authentication Manager/RSA SecurID Appliance 내의 호스트 이름은 로컬 네트워크의 유효한 IP 주소로 확인되어야 합니다.

다음 단계를 완료하십시오.

1. RSA 인증 관리자 호스트 모드 애플리케이션을 엽니다.
2. Agent **Host > Add Agent Host를 선택합니다**
.



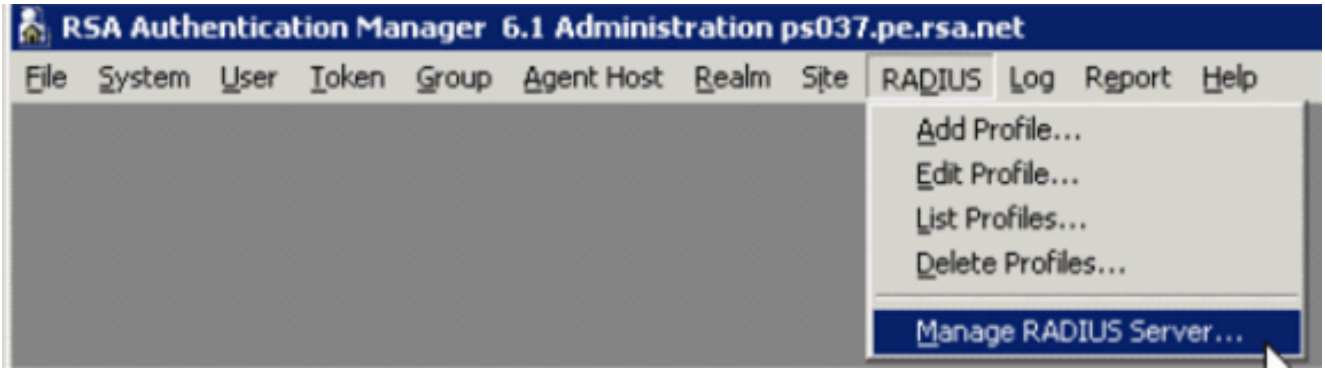


이 창이 표시됩니다.

3. WLC 호스트 이름(필요한 경우 확인 가능한 FQDN) 및 네트워크 주소에 대한 적절한 정보를 입력합니다.Communication **Server** for Agent type(에이전트 유형에 대한 통신 서버)을 선택하고 Open to All Locally Known Users(로컬로 알려진 모든 사용자에게 **열기) 확인란을 선택합니다**.

4. **확인**을 **클릭합니다**.
5. 메뉴에서 RADIUS > **Manage RADIUS** Server(RADIUS **서버 관리)를** 선택합니다

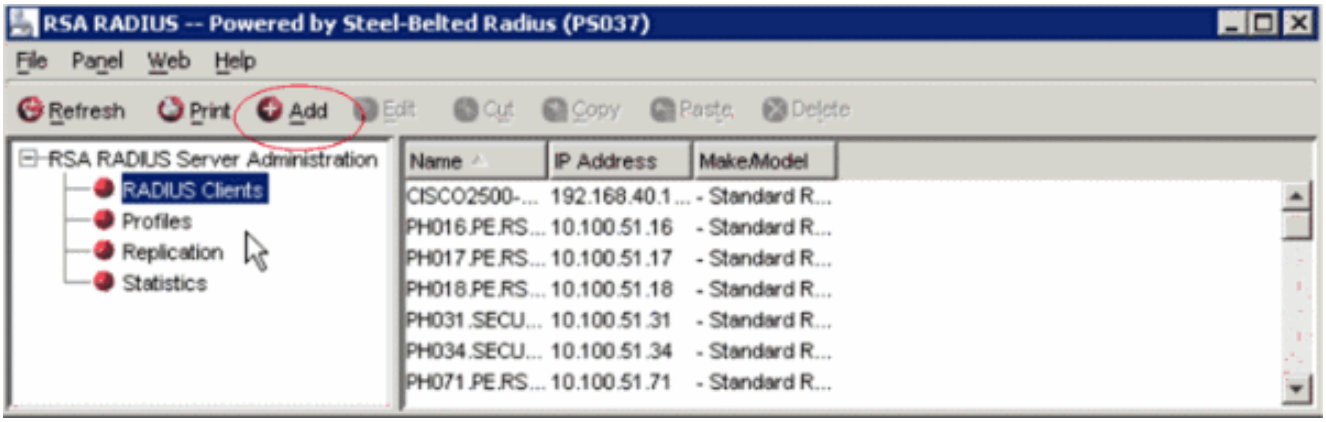
.



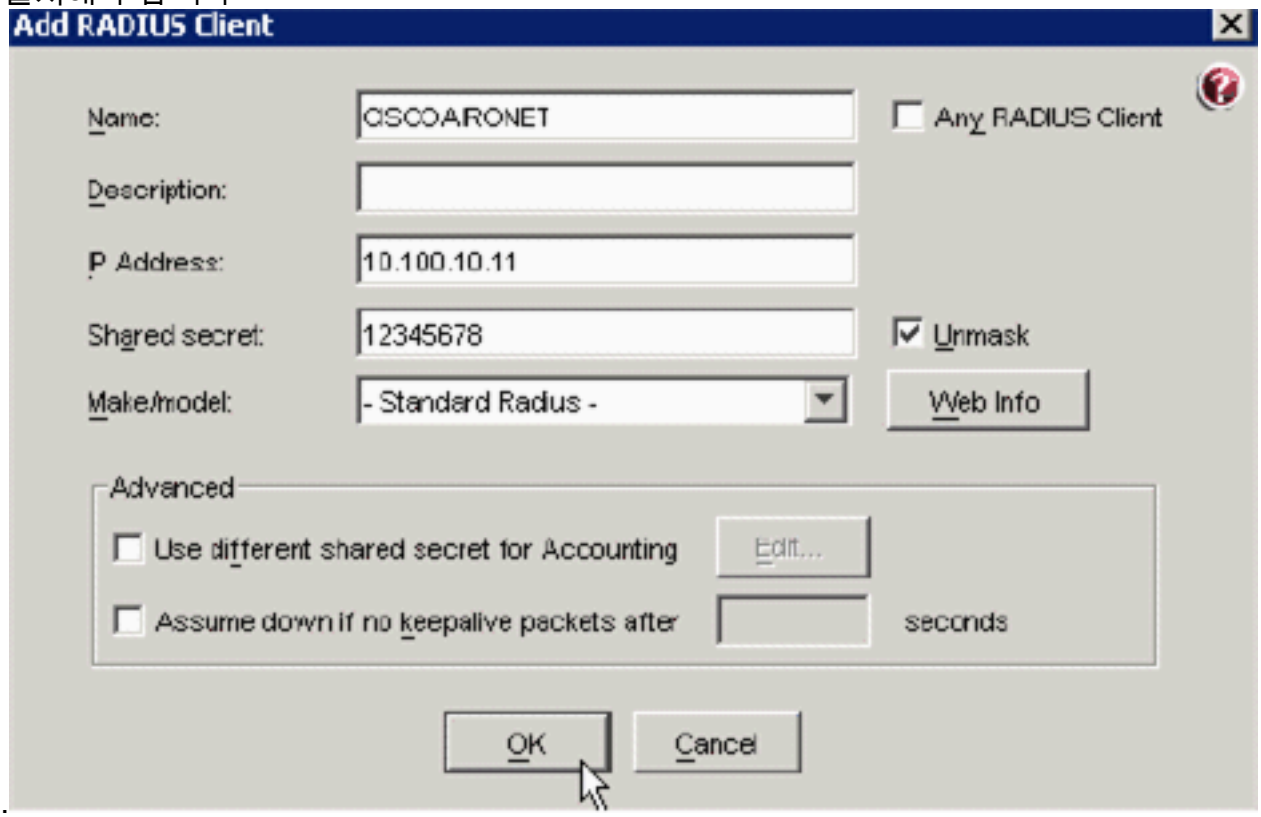
새 관리 창이 열립니다.

6. 이 창에서 **RADIUS Clients(RADIUS 클라이언트)**를 선택한 다음 Add(**추가)**를 클릭합니다

.



7. Cisco WLC에 대한 적절한 정보를 입력합니다.공유 암호는 Cisco WLC에 정의된 공유 암호와 일치해야 합니다



.

8. **확인**을 **클릭합니다**.

인증 에이전트 구성

다음 표는 ACS의 RSA 인증 에이전트 기능을 나타냅니다.

Partner Integration Overview	
Authentication Methods Supported	Native RSA SecurID Authentication, RADIUS, Both
List Library Version Used	5.0.3
RSA Authentication Manager Name Locking	Yes
RSA Authentication Manager Replica Support	Full Replica Support
Secondary RADIUS Server Support	N/A
Location of Node Secret on Agent	'None stored'
RSA Authentication Agent Host Type	Communication Server
RSA SecurID User Specification	Designated Users, All Users, Default Method
RSA SecurID Protection of Administrative Users	No
RSA Software Token API Integration	No
Use of Cached Domain Credentials	No

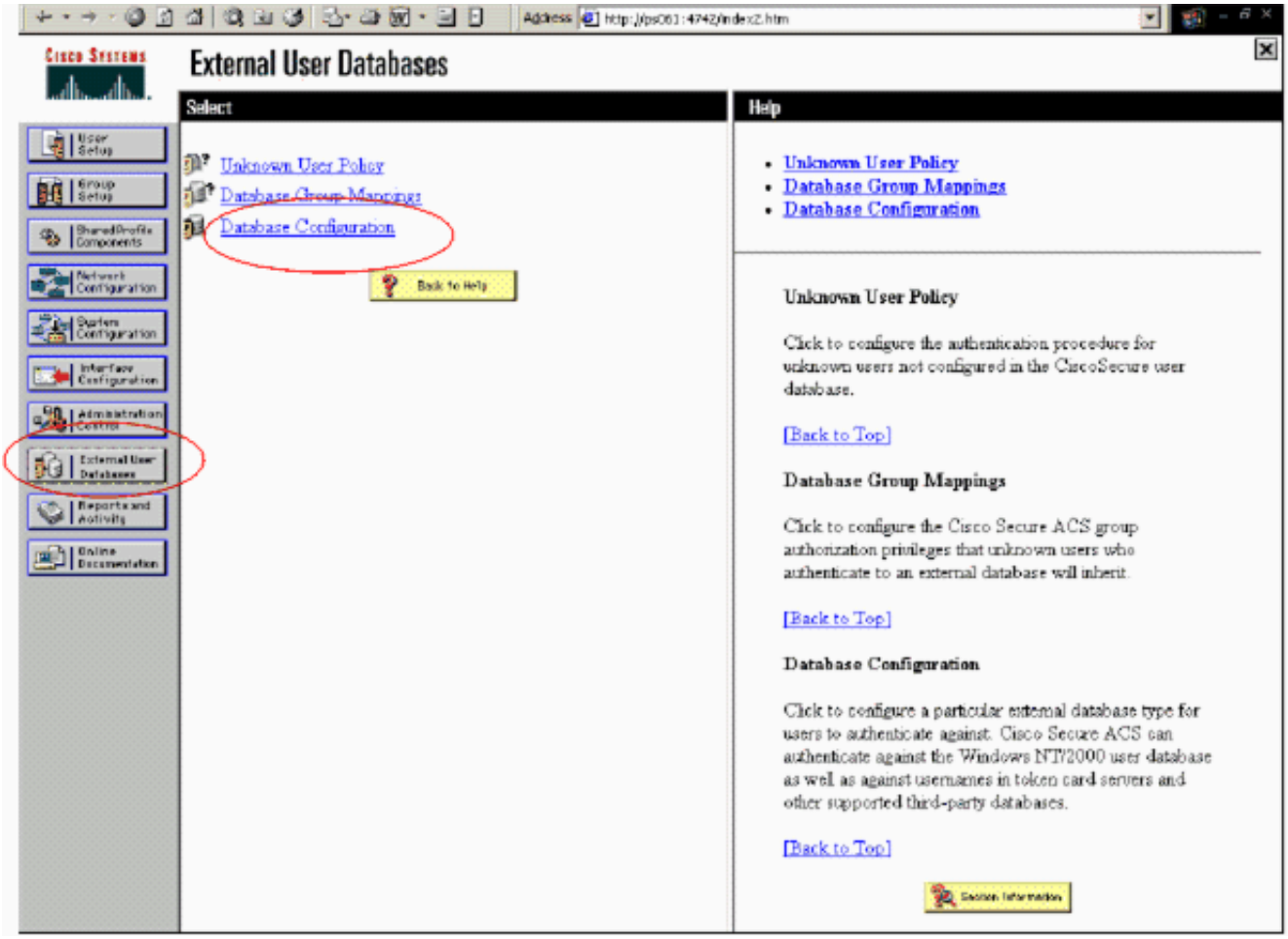
참고: RADIUS 서버를 구성하는 방법(RADIUS 서버를 사용할 RADIUS 서버인 경우)에 대해서는 RSA 인증 관리자에 포함된 RADIUS 설명서를 참조하십시오.

Cisco ACS 구성

RSA SecurID 인증 활성화

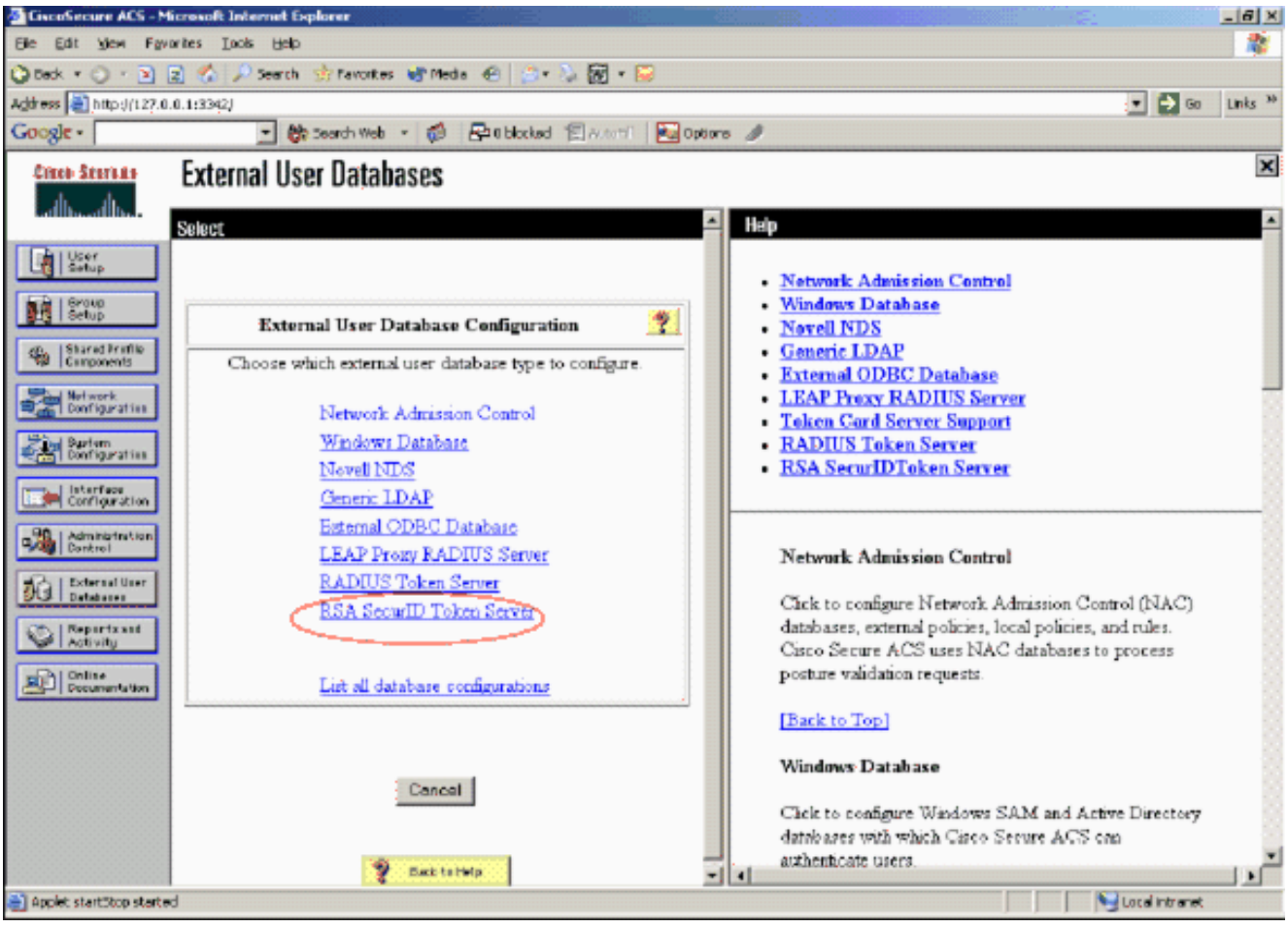
Cisco Secure ACS는 사용자의 RSA SecurID 인증을 지원합니다.Authentication Manager 6.1을 사용하여 사용자를 인증하도록 Cisco Secure ACS를 구성하려면 다음 단계를 완료합니다.

1. Cisco Secure ACS 서버와 동일한 시스템에 Windows용 RSA Authentication Agent 5.6 이상을 설치합니다.
2. 인증 에이전트의 테스트 인증 기능을 실행하여 연결을 확인합니다.
3. aceclnt.dll 파일을 RSA 서버 **c:\Program Files\RSA Security\RSA Authentication Manager\prog** 디렉토리에서 ACS 서버의 **c:\WINNT\system32** 디렉토리로 복사합니다.
4. 탐색 모음에서 **외부 사용자 데이터베이스**를 클릭합니다.그런 다음 [외부 데이터베이스] 페이지에서 [데이터베이스 구성]을 누릅니다
   .



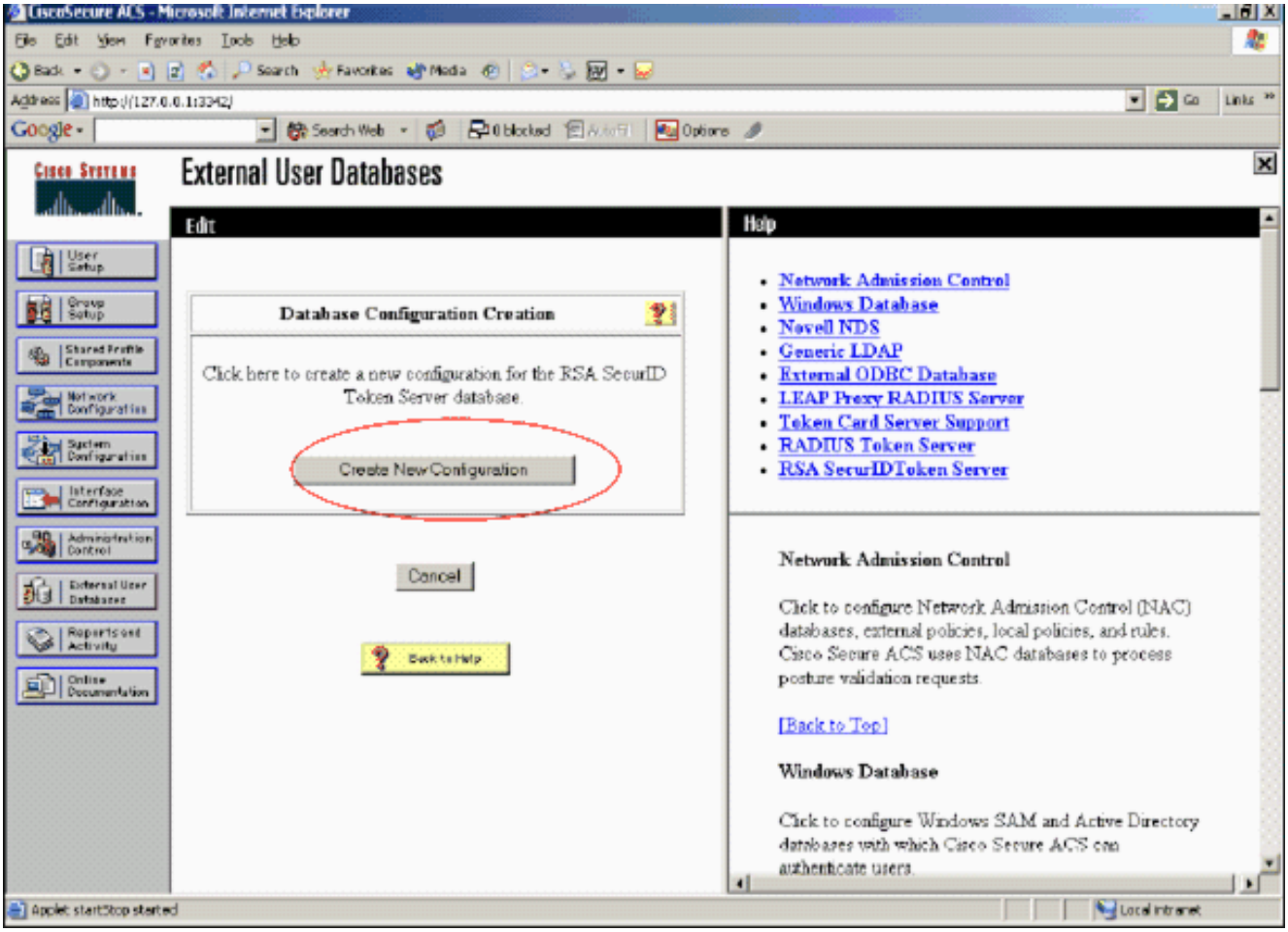
5. External User Database Configuration(외부 사용자 데이터베이스 컨피그레이션) 페이지에서 **RSA SecurID Token Server(RSA SecurID 토큰 서버)**를 클릭합니다

.



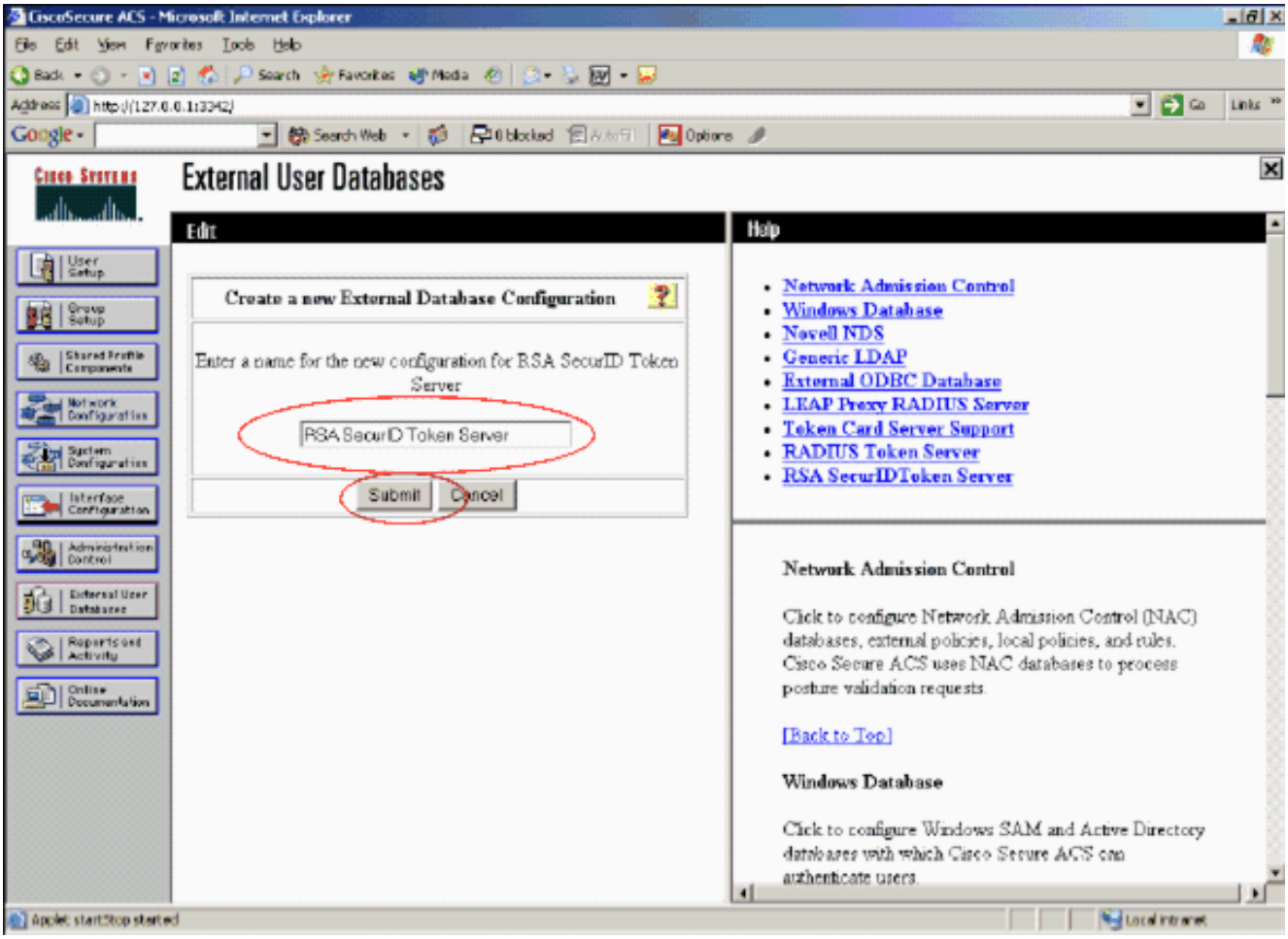
6. Create **New Configuration을 클릭합니다**

.



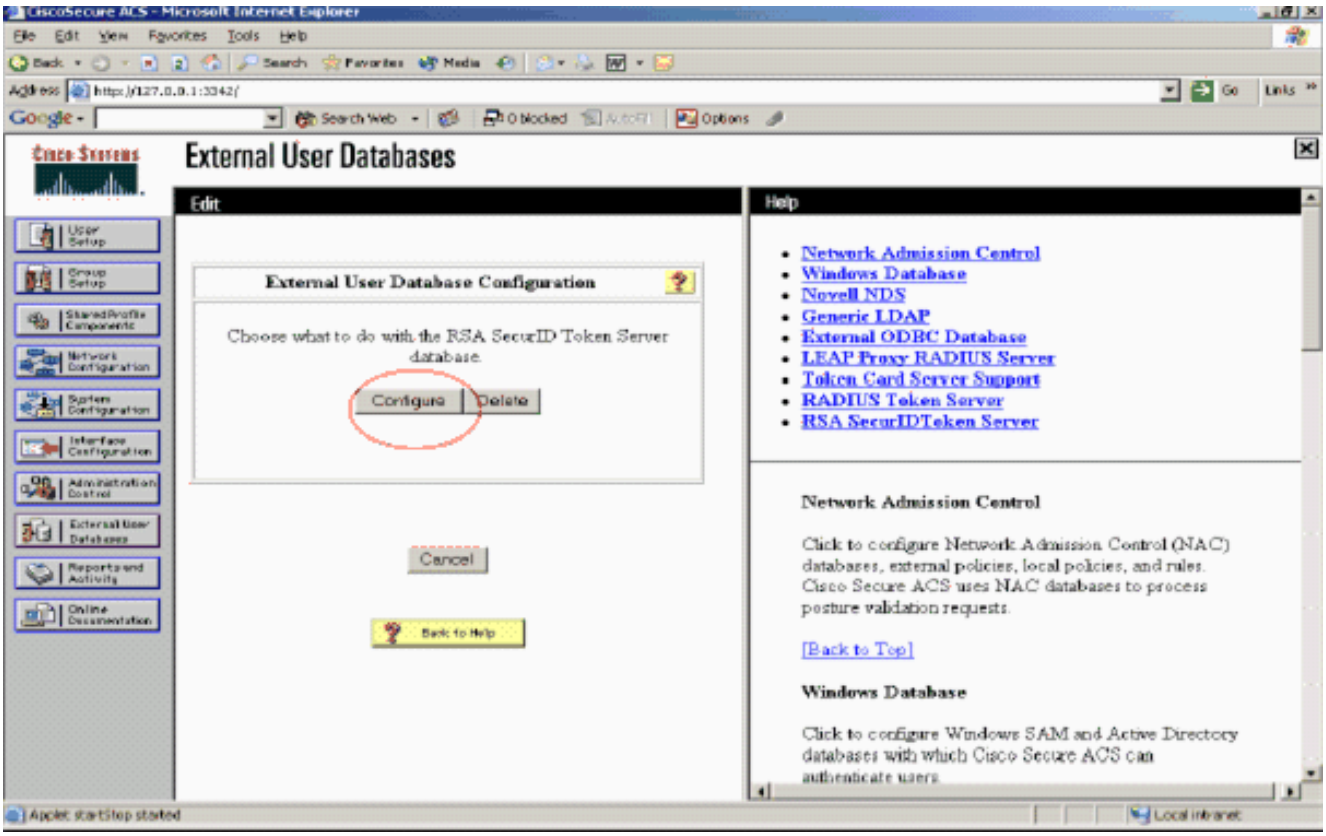
7. 이름을 입력한 다음 Submit(제출)을 **클릭합니다**

.



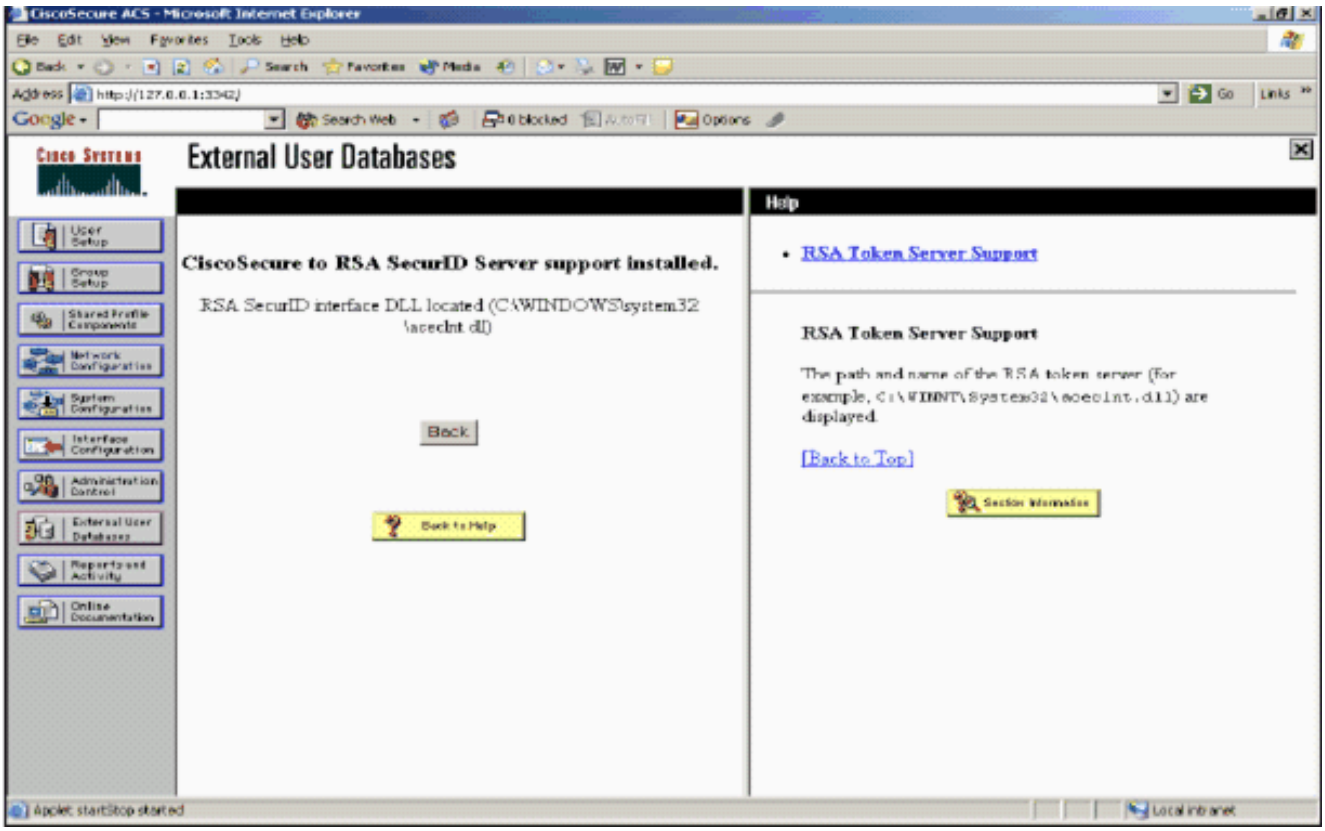
8. 구성을 **클릭합니다**

.



Cisco Secure ACS는 토큰 서버의 이름 및 인증자 DLL의 경로를 표시합니다.이 정보는 Cisco Secure ACS가 RSA 인증 에이전트에 연결할 수 있음을 확인합니다.알 수 없는 사용자 정책에 RSA SecurID 외부 사용자 데이터베이스를 추가하거나 인증을 위해 이 데이터베이스를 사용할 특정 사용자 계정을 할당할 수 있습니다

.

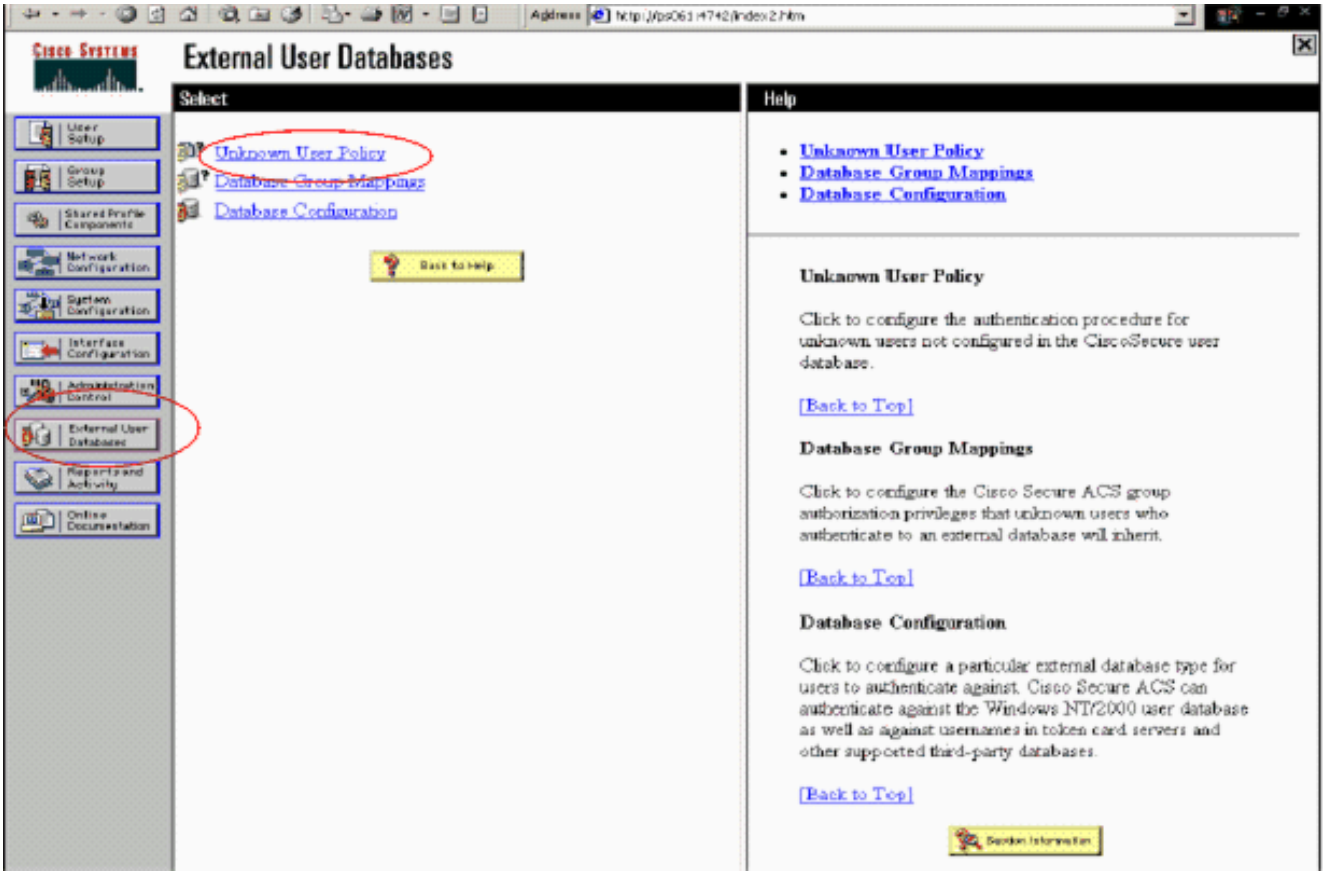


알 수 없는 사용자 정책에 RSA SecurID 인증 추가/구성

다음 단계를 완료하십시오.

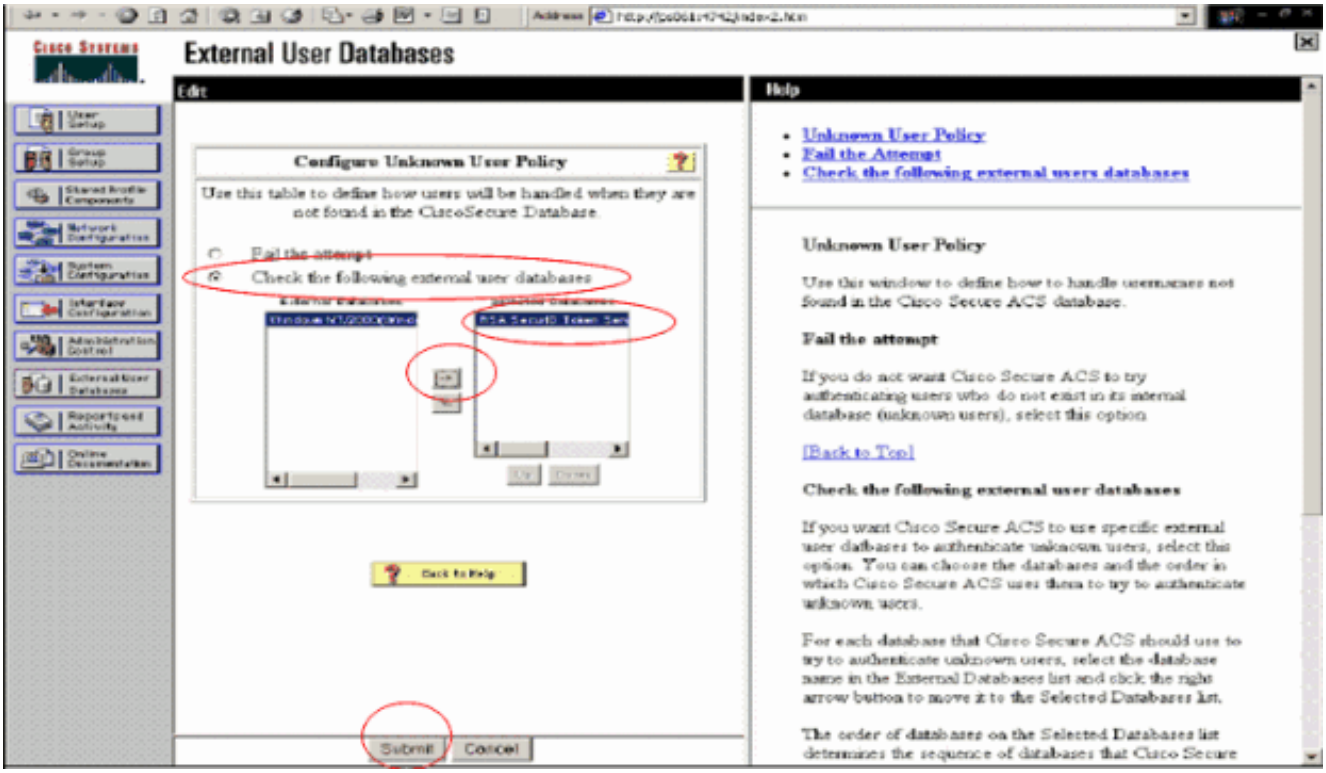
1. ACS 탐색 모음에서 **외부 사용자 데이터베이스 > 알 수 없는 사용자 정책을** 클릭합니다

.



2. Unknown **User Policy** 페이지에서 **Check the following external user databases(다음 외부 사용자 데이터베이스 확인)를** 선택하고 **RSA SecurID Token Server(RSA SecurID 토큰 서버)**를 강조 표시하고 Selected Databases(선택한 데이터베이스) 상자로 이동합니다.그런 다음 Submit(제출)을 **클릭합니다**

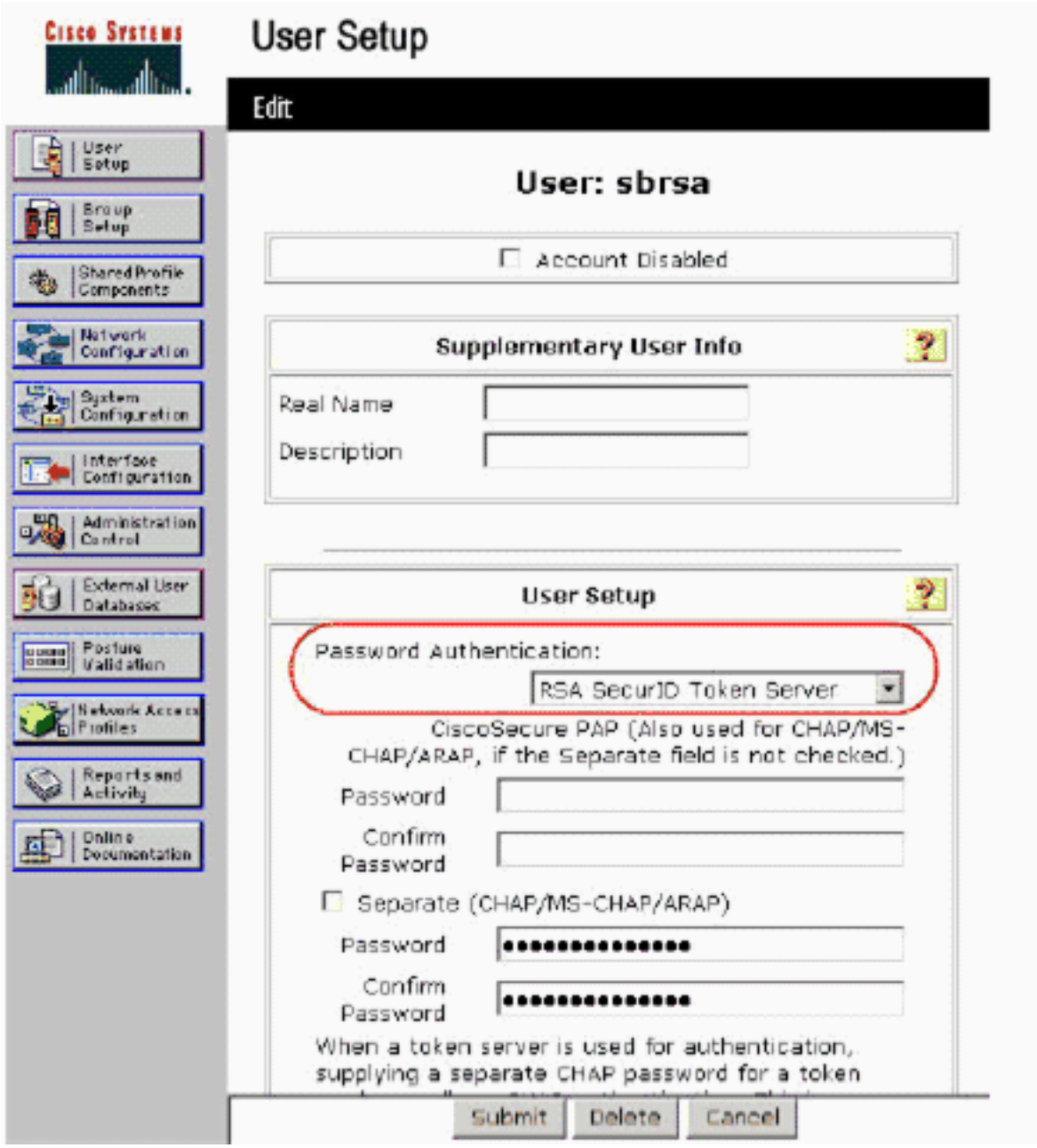
.



특정 사용자 계정에 대한 RSA SecurID 인증 추가/구성

다음 단계를 완료하십시오.

1. 기본 **ACS** 관리 GUI에서 User Setup을 클릭합니다.사용자 이름을 입력하고 **Add**(추가)를 클릭합니다. 또는 수정할 기존 사용자를 선택합니다.
2. User Setup(사용자 설정) > Password Authentication(비밀번호 인증)에서 **RSA SecurID Token Server(RSA SecurID 토큰 서버)를** 선택합니다.그런 다음 Submit(제출)을 **클릭합니다**

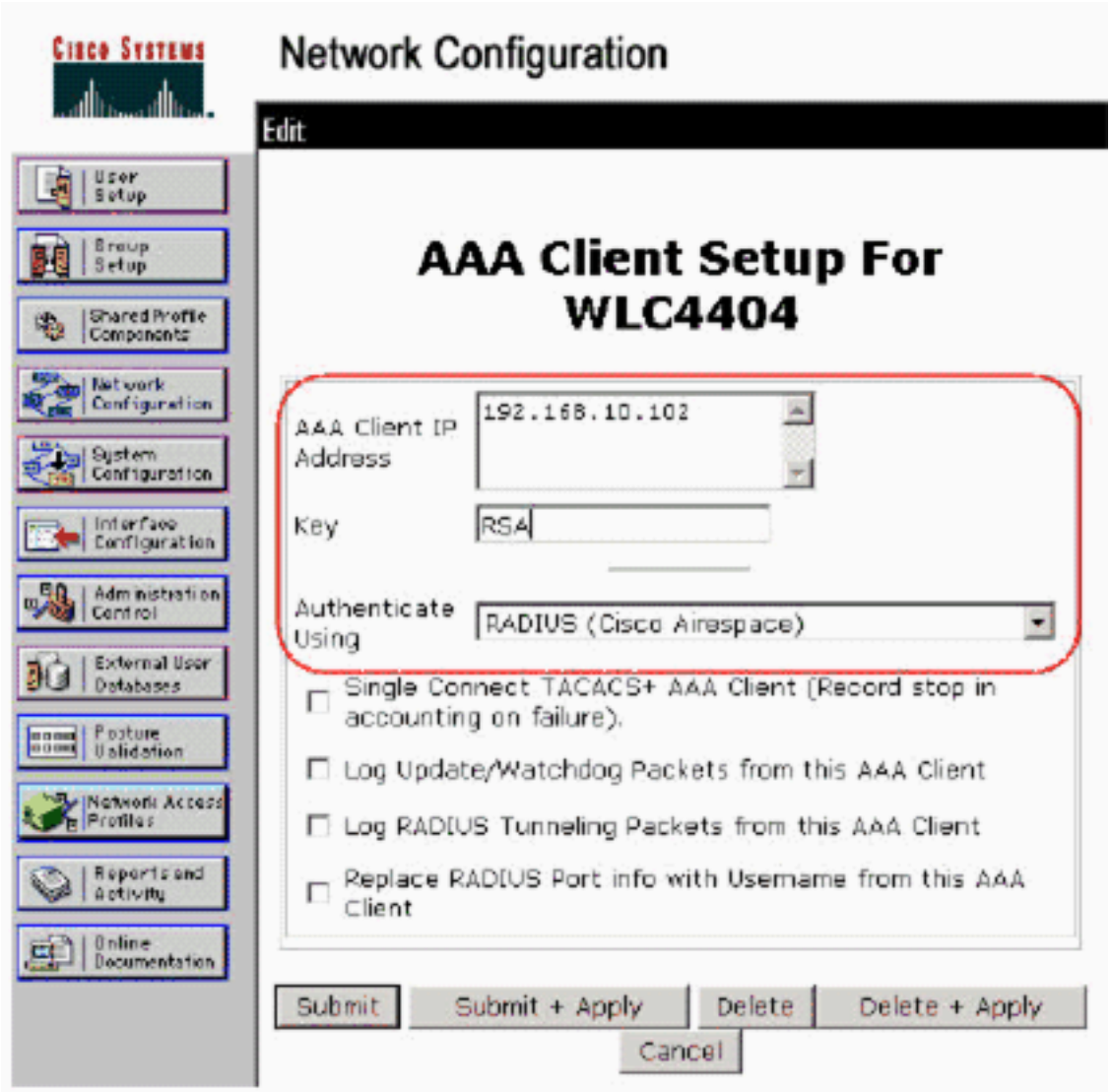


Cisco ACS에서 RADIUS 클라이언트 추가

Cisco ACS 서버 설치에는 ACS에 클라이언트 PEAP 인증을 전달하는 NAS의 역할을 하기 위해 WLC의 IP 주소가 필요합니다.

다음 단계를 완료하십시오.

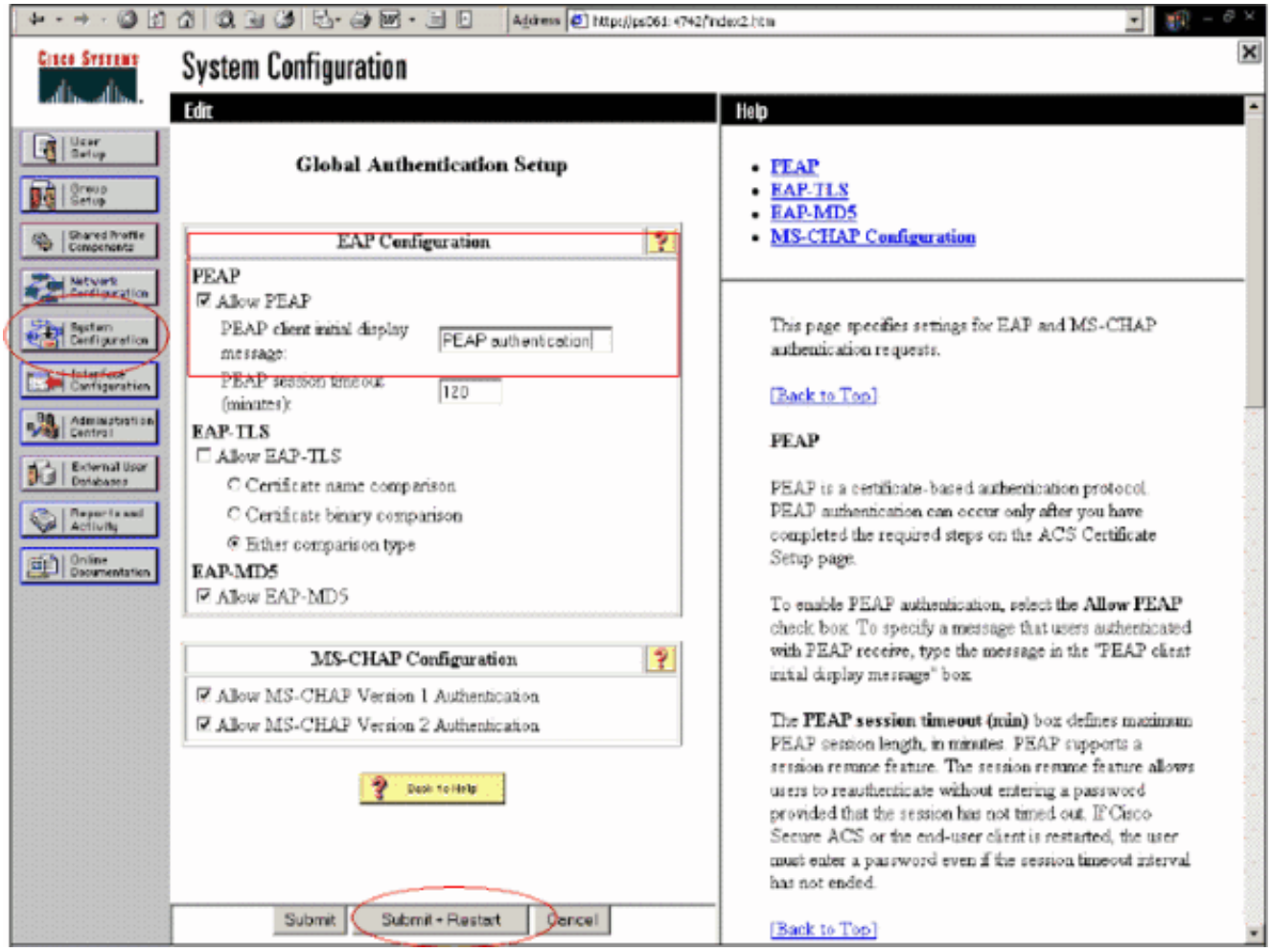
1. Network **Configuration(네트워크 컨피그레이션)**에서 사용할 WLC에 대한 AAA 클라이언트를 추가/수정합니다.AAA 클라이언트와 ACS 간에 사용되는 "공유 암호" 키(WLC에 공통)를 입력합니다.이 **AAA 클라이언트에 대해 Authenticate Using > RADIUS (Cisco Airespace)**를 선택합니다.그런 다음 Submit **+Apply**를 클릭합니다



.

2. RSA Keon Certificate Authority와 같이 신뢰할 수 있는 알려진 인증 기관에서 서버 인증서를 신청하여 설치합니다.이 프로세스에 대한 자세한 내용은 Cisco ACS와 함께 제공되는 설명서를 참조하십시오.RSA Certificate Manager를 사용하는 경우 RSA Keon Aironet 구현 가이드에서 추가 도움말을 볼 수 있습니다.계속하려면 이 작업을 완료해야 합니다.**참고:** 자체 서명 인증서도 사용할 수 있습니다.이러한 기능을 사용하는 방법은 Cisco Secure ACS 설명서를 참조하십시오.
3. System **Configuration(시스템 컨피그레이션) > Global Authentication Setup(전역 인증 설정**)에서 Allow PEAP authentication(PEAP 인증 **허용)** 확인란을 선택합니다

.



802.1x용 Cisco Wireless LAN Controller 구성

다음 단계를 완료하십시오.

1. WLC의 명령줄 인터페이스에 연결하여 Cisco Secure ACS Server에 연결하도록 구성할 수 있도록 컨트롤러를 구성합니다.
2. WLC에서 **config radius auth ip-address** 명령을 입력하여 인증을 위한 RADIUS 서버를 구성합니다.**참고:** RSA Authentication Manager RADIUS 서버로 테스트할 때 RSA Authentication Manager RADIUS 서버의 IP 주소를 입력합니다.Cisco ACS 서버로 테스트할 때 Cisco Secure ACS 서버의 IP 주소를 입력합니다.
3. WLC에서 **config radius auth port** 명령을 입력하여 인증을 위한 UDP 포트를 지정합니다.포트 1645 또는 1812는 기본적으로 RSA Authentication Manager 및 Cisco ACS 서버에서 모두 활성화되어 있습니다.
4. WLC에서 **config radius auth secret** 명령을 입력하여 WLC에서 공유 암호를 구성합니다.이 RADIUS 클라이언트의 RADIUS 서버에서 생성된 공유 암호와 일치해야 합니다.
5. 인증을 **활성화하려면 WLC에서 config radius auth enable** 명령을 입력합니다.원하는 경우 인증을 비활성화하려면 **config radius auth disable** 명령을 입력합니다.기본적으로 인증이 비활성화되어 있습니다.
6. WLC에서 원하는 WLAN에 적합한 레이어 2 보안 옵션을 선택합니다.
7. **show radius auth statistics** 및 **show radius summary** 명령을 사용하여 RADIUS 설정이 올바르게 구성되었는지 확인합니다.**참고:** EAP Request-timeout의 기본 타이머는 낮으므로 수정해야 할 수 있습니다.이 작업은 config **advanced eap request-timeout *<seconds>* 명령**을 사용하여 수행할 수 있습니다.또한 요구 사항에 따라 ID 요청 시간 제한을 조정하는 데 도움이 될 수 있습니다.이 작업은 config **advanced eap identity-request-timeout *<seconds>* 명령**을 사용하여

수행할 수 있습니다.

802.11 무선 클라이언트 구성

무선 하드웨어 및 클라이언트 서 플리 컨 트를 구성 하는 방법에 대한 자세한 설명은 다양한 Cisco 설명서를 참조 하십시오.

알려진 문제

다음은 RSA SecureID 인증에 대해 잘 알려진 몇 가지 문제입니다.

- RSA 소프트웨어 토큰.XP2에서 이 인증 형식을 사용하는 경우 새 핀 모드 및 다음 토큰 코드 모드가 지원되지 않습니다. (ACS-4.0.1-RSA-SW-CSCsc12614-CSCsd41866.zip의 결과 고정)
- ACS 구현이 이전 버전이거나 위의 패치가 없는 경우, 사용자가 "Enabled;New PIN Mode"에서 "Enabled"로 전환할 때까지 클라이언트를 인증할 수 없습니다.사용자가 비무선 인증을 완료하도록 하거나 "테스트 인증" RSA 애플리케이션을 사용하여 이를 수행할 수 있습니다.
- 4자리/영숫자 PIN을 거부합니다.새 핀 모드에서 사용자가 PIN 정책을 위반할 경우 인증 프로세스가 실패하고 사용자는 그 방법과 이유를 알지 못합니다.일반적으로 사용자가 정책에 반대하면 PIN이 거부되었다는 메시지가 전송되고 사용자에게 PIN 정책이 무엇인지 다시 표시하는 동안 다시 메시지가 표시됩니다(예를 들어, PIN 정책이 5-7자리이지만 사용자가 4자리를 입력하는 경우).

관련 정보

- ACS를 기반으로 WLC를 사용하여 동적 VLAN 할당 Active Directory 그룹 매핑 구성 예
- WLC 컨피그레이션이 포함된 무선 LAN을 통한 클라이언트 VPN 예
- 무선 LAN 컨트롤러 인증 컨피그레이션 예
- 무선 LAN 컨트롤러 및 외부 RADIUS 서버 구성을 통한 EAP-FAST 인증 예
- SDM을 통한 고정 ISR의 무선 인증 유형 구성 예
- 고정 ISR 컨피그레이션의 무선 인증 유형 예
- Cisco Protected Extensible Authentication Protocol
- RADIUS 서버를 사용한 EAP 인증
- 기술 지원 및 문서 – Cisco Systems