보안 유선 액세스

Cisco ISE의 네트워크 디바이스 정의

스위치 또는 라우터와 같은 네트워크 디바이스는 AAA(Authentication, Authorization, Accounting) 서비스 요청이 Cisco ISE로 전송될 때 사용되는 AAA 클라이언트입니다. Cisco ISE와 네트워크 디바이스 간의 상호 작용을 활성화하려면 Cisco ISE에서 네트워크 디바이스를 정의합니다.

프로파일링 서비스에 대해 RADIUS 또는 TACACS AAA, SNMP(Simple Network Management Protocol)용 네트워크 디바이스를 구성하여 프로파일링 엔드포인트용 Cisco Discovery Protocol 및 LLDP(Link Layer Discovery Protocol) 속성과 Cisco TrustSec 디바이스용 TrustSec 속성을 수집할 수 있습니다. Cisco ISE에 정의되지 않은 네트워크 디바이스는 Cisco ISE에서 AAA 서비스를 받을 수 없습니다.

네트워크 디바이스 정의에서는 다음을 수행합니다.

- 네트워크 디바이스에 적합한 벤더 프로파일을 선택합니다. 프로파일에는 URL 리디렉션 및 Change of Authorization용 설정과 같이 디바이스용으로 미리 정의된 컨피그레이션이 포함됩니다.
- RADIUS 인증용 RADIUS 프로토콜을 구성합니다. Cisco ISE가 네트워크 디바이스에서 RADIUS 요청을 받으면 해당 디바이스 정의를 찾아 구성된 공유 암호를 검색합니다. Cisco ISE가 디바이스 정의를 찾으면 해당 디바이스에 구성된 공유 암호를 가져와 액세스 인증을 위해 요청의 공유 암호와 일치하는지 확인합니다. 공유 암호가 일치하면 RADIUS 서버는 정책과 컨피그레이션을 기준으로 하여 요청을 추가로 처리합니다. 공유 암호가 일치하지 않으면 네트워크 디바이스에 거부 응답이 전송됩니다. 실패 이유를 제공하는 실패한 인증 보고서가 생성됩니다.

- TACACS+ 인증용 TACACS+ 프로토콜을 구성합니다. Cisco ISE는 네트워크 디바이스에서 TACACS+ 요청을 받으면 해당 디바이스 정의를 찾아 구성된 공유 암호를 검색합니다. 디바이스 정의가 발견되면 디바이스에 구성된 공유 암호를 가져와 액세스 인증을 위해 요청의 공유 암호와 일치하는지 확인합니다. 공유 암호가 일치하면 TACACS+ 서버는 정책과 컨피그레이션을 기준으로 하여 요청을 추가로 처리합니다. 일치하지 않으면 네트워크 디바이스에 거부 응답이 전송됩니다. 실패 이유를 제공하는 실패한 인증 보고서가 생성됩니다.
- 네트워크 디바이스 정의에서 프로파일링 서비스가 네트워크 디바이스 및 네트워크 디바이스에 연결된 프로파일 엔드포인트와 통신하도록 SNMP(Simple Network Management Protocol)를 구성할 수 있습니다.
- Cisco Trustsec 솔루션에 속할 수 있는 TrustSec 지원 디바이스의 요청을 처리하도록 Cisco ISE에서 Cisco TrustSec 지원 디바이스를 정의해야 합니다. Cisco TrustSec 솔루션을 지원하는 모든 스위치는 Cisco TrustSec 지원 디바이스입니다.

  Cisco TrustSec 디바이스는 IP 주소를 사용하지 않습니다. 대신 Cisco TrustSec 디바이스가 Cisco ISE와 통신할 수 있도록 다른 설정을 정의해야 합니다.

  Cisco TrustSec 지원 디바이스는 TrustSec 속성을 사용하여 Cisco ISE와 통신합니다. Nexus 7000 Series 스위치, Catalyst 6000 Series 스위치, Catalyst 4000 Series 스위치 및 Catalyst 3000 Series 스위치와 같은 Cisco TrustSec 지원 디바이스는 Cisco TrustSec 디바이스를 추가하는 동안 정의된 Trustsec 속성을 사용하여 인증됩니다.

참고 Cisco ISE에서 네트워크 디바이스를 구성할 때는 공유 암호에 백슬래시(\)를 포함하지 않는 것이 좋습니다. Cisco ISE를 업그레이드할 때 백슬래시가 공유 암호에 표시되지 않기 때문입니다. 단, Cisco ISE를 업그레이드하는 대신 재이미지화하는 경우 백슬래시가 공유 암호에 나타납니다.

Cisco ISE의 기본 네트워크 디바이스 정의

Cisco ISE는 RADIUS 및 TACACS 인증을 위한 기본 디바이스 정의를 지원합니다. Cisco ISE가 특정 IP 주소에 대한 디바이스 정의를 발견하지 못하는 경우에 사용할 수 있는 기본 네트워크 디바이스를 정의할 수 있습니다. 이 기능을 사용하면 새로 프로비저닝된 디바이스에 대한 기본 RADIUS 또는 TACACS 공유 암호 및 액세스 레벨을 정의할 수 있습니다.

참고 기본 RADIUS 및 TACACS 인증에 대해서만 기본 디바이스 정의를 추가하는 것이 좋습니다. 고급 플로우에서는 각 네트워크 디바이스에 대한 별도의 디바이스 정의를 추가해야 합니다.

Cisco ISE는 네트워크 디바이스에서 RADIUS 또는 TACACS 요청을 수신하면 해당 디바이스 정의를 찾아 네트워크 디바이스 정의에 구성된 공유 암호를 검색합니다.

RADIUS 또는 TACACS 요청이 수신되는 경우 Cisco ISE는 다음 절차를 수행합니다.

1. 요청의 IP 주소와 일치하는 특정 IP 주소를 찾습니다.
2. 범위를 조회하여 요청의 IP 주소가 지정된 범위 안에 포함되는지 확인합니다.

3. 1단계와 2단계 모두 실패하는 경우 기본 디바이스 정의(정의된 경우)를 사용하여 요청을 처리합니다.

Cisco ISE는 해당 디바이스의 디바이스 정의에 구성된 공유 암호를 가져온 다음 RADIUS 또는 TACACS 요청의 공유 암호와 일치하는지 확인하여 액세스를 인증합니다. 디바이스 정의를 찾을 수 없는 경우 Cisco ISE는 기본 네트워크 디바이스 정의에서 공유 암호를 가져와 RADIUS 또는 TACACS 요청을 처리합니다.

네트워크 디바이스

이들 창에서 Cisco ISE에 네트워크 디바이스를 추가하고 관리할 수 있습니다.

네트워크 디바이스 정의 설정

다음 표에서는 Cisco ISE에서 네트워크 액세스 디바이스를 구성하는 데 사용할 수 있는 **Network Devices(**네트워크 디바이스**)** 창의 필드에 대해 설명합니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Network Resources(**네트워크 리소스**)** > **Network Devices(**네트워크 디바이스**)**입니다. 그런 다음 **Add(**추가**)**를 클릭합니다.

네트워크 디바이스 설정

다음 표에서는 **New Network Devices(**새 네트워크 디바이스**)** 창의 필드에 대해 설명합니다.

표 ***1:*** 네트워크 디바이스 설정

필드 이름	설명
Name(이름**)**	네트워크 디바이스의 이름을 입력합니다. 디바이스의 호스트 이름과 다른, 네트워크 디바이스를 설명하는 이름을 입력할 수 있습니다. 디바이스 이름은 논리적 식별자입니다. 참고 디바이스를 구성한 후에는 그 이름을 편집할 수 없습니다.
Description(설명**)**	디바이스에 대한 설명을 입력합니다.

필드 이름	설명
IP 주소 또는 **IP** 범위	드롭다운 목록에서 다음 중 하나를 선택하고 표시되는 필드에 필요한 값을 입력합니다. • **IP Address(IP** 주소**)**: 단일 IP 주소(IPv4 또는 IPv6 주소)와 서브넷 마스크를 입력합니다. • **IP Range(IP** 범위**)**: 필요한 IPv4 주소 범위를 입력합니다. 인증 중에 IP 주소를 제외하려면 **Exclude(**제외**)** 필드에 IP 주소 또는 IP 주소 범위를 입력합니다. IP 주소 및 서브넷 마스크 또는 IP 주소 범위를 정의할 때의 지침은 다음과 같습니다. • 특정 IP 주소를 정의하거나 서브넷 마스크가 포함된 IP 범위를 정의할 수 있습니다. 디바이스 A에 IP 주소 범위가 정의되어 있으면 디바이스 A에 정의된 범위의 개별 주소를 사용하여 다른 디바이스 B를 구성할 수 있습니다. • 모든 옥텟에서 IP 주소 범위를 정의할 수 있습니다. IP 주소 범위를 지정하는 경우 하이픈(-)을 사용하거나 별표(*)를 와일드카드로 사용할 수 있습니다. 예를 들어 *.*.*.*, 1-10.1-10.1-10.1-10 또는 10-11.*.5.10-15와 같이 지정할 수 있습니다. • IP 주소 범위의 일부가 이미 추가된 경우에는 구성된 범위에서 이를 제외할 수 있습니다. 예를 들어 10.197.65.*/10.197.65.1과 같이 지정하여 10.197.65.*에서 10.197.65.1를 제외할 수 있습니다. • 동일한 특정 IP 주소를 사용하여 두 개의 디바이스를 정의할 수는 없습니다. • 동일한 IP 범위를 사용하여 두 개의 디바이스를 정의할 수는 없습니다. IP 범위가 일부분 또는 완전히 겹쳐서는 안 됩니다.

필드 이름	설명
Device Profile(디바이스 프로파일**)**	드롭다운 목록에서 네트워크 디바이스의 벤더를 선택합니다. 드롭다운 목록 옆의 툴팁을 사용하여 선택한 벤더의 네트워크 디바이스가 지원하는 플로우 및 서비스를 확인할 수 있습니다. 툴팁에는 디바이스에서 사용되는 URL 리디렉션의 유형 및 RADIUS CoA 포트도 표시됩니다. 이러한 속성은 디바이스 유형의 네트워크 디바이스 프로파일에 정의되어 있습니다.
Model Name(모델 이름**)**	드롭다운 목록에서 디바이스 모델을 선택합니다. 규칙 기반 정책에서 조건을 확인하는 동안 모델 이름을 매개변수 중 하나로 사용합니다. 이 속성은 디바이스 사전에 있습니다.
Software Version(소프트웨어 버전**)**	드롭다운 목록에서 네트워크 디바이스에서 실행되는 소프트웨어의 버전을 선택합니다. 규칙 기반 정책에서 조건을 확인하는 동안 소프트웨어 버전을 매개변수 중 하나로 사용할 수 있습니다. 이 속성은 디바이스 사전에 있습니다.
Network Device Group(네트워크 디바이스 그룹**)**	**Network Device Group(**네트워크 디바이스 그룹**)** 영역의 **Location(**위치**)**, **IPSEC** 및 **Device Type(**디바이스 유형**)** 드롭다운 목록에서 필요한 값을 선택합니다. 그룹에 구체적으로 할당하지 않는 디바이스는 기본 디바이스 그룹(루트 네트워크 디바이스 그룹)에 포함됩니다. 기본 디바이스 그룹은 위치 기준 **All Locations(**모든 위치**)** 및 디바이스 유형 기준 **All Device Types(**모든 디바이스 유형**)**입니다.

RADIUS 인증 설정

다음 표에서는 **RADIUS** 인증 설정 영역의 필드에 대해 설명합니다.

표 ***2: RADIUS*** 인증 설정 영역의 필드

필드 이름	사용 지침
RADIUS UDP Settings(RADIUS UDP 설정**)**	
Protocol(프로토콜**)**	**RADIUS**를 선택한 프로토콜로 표시합니다.

필드 이름	사용 지침
Shared Secret(공유 암호**)**	네트워크 디바이스의 공유 암호를 입력합니다. 공유 암호는 **radius-host** 명령(**pac** 옵션 포함)을 사용하여 네트워크 디바이스에 구성된 키입니다. 참고 공유 암호 길이는 **Device Security Settings(**디바이스 보안 설정**)** 창(**Administration(**관리**) > Network Resources(**네트워크 리소스**) > Network Devices(**네트워크 디바이스**) > Device Security Settings(**네트워크 보안 설정**))** 창의 **Minimum RADIUS Shared Secret Length(**최소 **RADIUS** 공유 암호 길이**)** 필드에 구성된 값보다 크거나 같아야 합니다. RADIUS 서버의 경우 모범 사례는 22자입니다. 신규 설치 및 업그레이드된 구축의 경우 공유 암호 길이는 기본적으로 4자입니다. **Device Security Settings(**디바이스 보안 설정**)** 창에서 이 값을 변경할 수 있습니다.

필드 이름	사용 지침
Use Second Shared Secret(두 번째 공유 암호 사용**)**	네트워크 디바이스 및 Cisco ISE에서 사용할 두 번째 공유 암호를 지정합니다. 참고 Cisco TrustSec 디바이스는 이중 공유 암호(키)를 활용할 수 있지만 Cisco ISE에서 전송되는 Cisco TrustSec CoA 패킷은 항상 첫 번째 공유 암호(키)를 사용합니다. 두 번째 공유 암호를 활성화하려면 Cisco TrustSec CoA 패킷을 Cisco TrustSec 디바이스로 전송할 Cisco ISE 노드를 선택합니다. **Work Centers(**작업 센터**)** > **Device Administration(**디바이스 관리**)** > **Network Resources(**네트워크 리소스**)** > **Network Devices(**네트워크 디바이스**)** > **Add(**추가**)** > **Advanced TrustSec Settings(**고급 **TrustSec** 설정**)** 창에 있는 **Send From(**전송 위치**)** 드롭다운 목록에서 이 작업에 사용할 Cisco ISE 노드를 구성합니다. PAN(Primary Administration Node) 또는 PSN(Policy Service Node)을 선택할 수 있습니다. 선택한 PSN 노드가 작동 중지된 경우 PAN은 Cisco TrustSec CoA 패킷을 Cisco TrustSec 디바이스로 전송합니다. 참고 RADIUS 액세스 요청에 대한 두 번째 공유 암호 기능은 **Message-Authenticator** 필드를 포함하는 패킷에 대해서만 작동합니다.

필드 이름	사용 지침
CoA Port(CoA 포트**)**	RADIUS CoA에 사용할 포트를 지정합니다. 디바이스의 기본 CoA 포트는 네트워크 디바이스에 대해 구성된 네트워크 디바이스 프로파일(**Administration(**관리**)** > **Network Resources(**네트워크 리소스**)** > **Network Device Profiles(**네트워크 디바이스 프로파일**)** > **Network Resources(**네트워크 리소스**)** > **Network Device Profiles(**네트워크 디바이스 프로파일)에 정의됩니다. 기본 CoA 포트를 사용하려면 **Set To Default(**기본값으로 설정**)** 버튼을 클릭합니다. 참고 **Network Devices(**네트워크 디바이스**)** 창(**Administration(**관리**)** > **Network Resources(**네트워크 리소스**)** > **Network Devices(**네트워크 디바이스**))**의 **RADIUS Authentication Settings(RADIUS** 인증 설정**)**에 지정된 CoA 포트를 수정하는 경우 **Network Device Profile(**네트워크 디바이스 프로파일**)** 창(**Administration(**관리**)** > **Network Resources(**네트워크 리소스**)** > **Network Device Profiles(**네트워크 디바이스 프로파일**))**의 해당 프로파일에도 동일한 CoA 포트를 지정하십시오.
RADIUS DTLS Settings(RADIUS DTLS 설정**)**	
DTLS Required(DTLS 필수**)**	**DTLS Required(DLTS** 필수**)** 확인란을 선택하면 Cisco ISE에서 이 디바이스의 DTLS 요청만 처리합니다. 이 옵션을 비활성화하면 Cisco ISE에서 이 디바이스의 UDP 요청과 DTLS 요청을 모두 처리합니다. RADIUS DTLS는 SSL(Secure Sockets Layer) 터널 설정 및 RADIUS 통신을 위한 향상된 보안을 제공합니다.
Shared Secret(공유 암호**)**	RADIUS DTLS에 사용되는 공유 암호를 표시합니다. 이 값은 고정되어 있으며 MD5(Message Digest 5) 무결성 확인을 처리하는 데 사용됩니다.
CoA Port(CoA 포트**)**	RADIUS DTLS CoA에 사용할 포트를 지정합니다.
Issuer CA of ISE Certificates for CoA(CoA의 **ISE** 인증서에 대한 발급자 **CA)**	드롭다운 목록에서 RADIUS DTLS CoA에 사용할 CA(Certificate Authority)를 선택합니다.

필드 이름	사용 지침
DNS Name(DNS 이름**)**	네트워크 디바이스의 DNS 이름을 입력합니다. **RADIUS Settings(RADIUS** 설정**)** 창 (**Administration(**관리**)** > **System(**시스템**)** > **Settings(**설정**)** > **Protocols(**프로토콜**)** > **RADIUS**)에서 **Enable RADIUS/DTLS Client Identity Verification(RADIUS/DTLS** 클라이언트 **ID** 확인 활성화**)** 옵션이 활성화된 경우 Cisco ISE는 이 DNS 이름을 클라이언트 인증서에 지정된 DNS 이름과 비교하여 네트워크 디바이스의 ID를 확인합니다.
General Settings(일반 설정**)**	
Enable KeyWrap(KeyWrap 활성화**)**	네트워크 디바이스에서 KeyWrap 알고리즘이 지원되는 경우에만 **Enable KeyWrap(KeyWrap** 활성화**)** 확인란을 선택합니다. 이 옵션은 AES KeyWrap 알고리즘을 통해 RADIUS 보안을 강화하는 데 사용됩니다. 참고 FIPS 모드에서 Cisco ISE를 실행할 때는 네트워크 디바이스에서 KeyWrap을 활성화해야 합니다.
Key Encryption Key(키 암호화 키**)**	세션 암호화(비밀 유지)에 사용되는 암호화 키를 입력합니다.
Message Authenticator Code Key(메시지 인증자 코드 키**)**	RADIUS 메시지에 대한 키 HMAC(Hashed Message Authentication Code) 계산에 사용되는 키를 입력합니다.

필드 이름	사용 지침
Key Input Format(키 입력 형식**)**	다음 형식 중 하나에 해당하는 라디오 버튼을 클릭합니다. • **ASCII**: **Key Encryption Key(**키 암호화 키**)** 필드에 입력하는 값의 길이는 16자(바이트)여야 하며 **Message Authenticator Code Key(**메시지 인증자 코드 키**)** 필드에 입력하는 값의 길이는 20자(바이트)여야 합니다. • **Hexadecimal**: **Key Encryption Key(**키 암호화 키**)** 필드에 입력하는 값의 길이는 32자(바이트)여야 하며 **Message Authenticator Code Key(**메시지 인증자 코드 키**)** 필드에 입력하는 값의 길이는 40자(바이트)여야 합니다. Cisco ISE FIPS 암호화 키를 입력하는 데 사용할 키 입력 형식을 무선 LAN 컨트롤러에서 사용 가능한 구성과 일치하도록 지정할 수 있습니다. 이 값은 키의 정확한(전체) 길이로 지정해야 하며 더 짧은 값은 지정할 수 없습니다.

TACACS 인증 설정

표 ***3: TACACS*** 인증 설정 영역의 필드

필드 이름	사용 지침
Shared Secret(공유 암호**)**	TACACS+ 프로토콜을 활성화할 때 네트워크 디바이스에 할당된 텍스트 문자열입니다. 네트워크 디바이스가 사용자 이름과 비밀번호를 인증하기 전에 사용자가 텍스트를 입력해야 합니다. 사용자가 공유 암호를 제공할 때까지는 연결이 거부됩니다.
Retired Shared Secret is Active(사용 중단된 공유 암호가 활성 상태임**)**	사용 중단 기간이 활성인 경우 표시됩니다.
Retire(사용 중단**)**	기존 공유 암호를 종료하는 대신 사용 중단합니다. **Retire(**사용 중단**)**를 클릭하면 메시지 상자가 표시됩니다. **Yes(**예**)** 또는 **No(**아니요**)**를 클릭할 수 있습니다.

필드 이름	사용 지침
Remaining Retired Period(남은 사용 중단 기간**)**	(**Retire(**사용 중단**)** 메시지 상자에서 **Yes(**예**)**를 선택한 경우에만 사용 가능함) **Work Centers(**작업 센터**)** > **Device Administration(**디바이스 관리**)** > **Settings(**설정**)** > **Connection Settings(**연결 설정**)** > **Default Shared Secret Retirement Period(**기본 공유 암호 사용 중단 기간**)** 탐색 경로에 지정되어 있는 기본값이 표시됩니다. 기본값은 변경할 수 있습니다. 그러면 새 공유 암호를 입력할 수 있습니다. 이전 공유 암호는 지정된 기간(일) 동안 활성 상태로 유지됩니다.
End(종료**)**	(**Retire(**사용 중단**)** 메시지 상자에서 **Yes(**예**)**를 선택한 경우에만 사용 가능함) 사용 중단 기간을 종료하고 이전 공유 암호 사용을 중단합니다.
Enable Single Connect Mode(단일 연결 모드 활성화**)**	네트워크 디바이스와의 모든 TACACS+ 통신에 단일 TCP 연결을 사용하려면 **Enable Single Connect Mode(**단일 연결 모드 활성화**)** 확인란을 선택합니다. 다음 중 하나의 옵션에 해당하는 라디오 버튼을 클릭합니다. • **Legacy Cisco Devices(**레거시 **Cisco** 디바이스**)** • **TACACS Draft Compliance Single Connect Support(TACACS+** 초안 규정 준수 단일 연결 지원**)** **Single Connect Mode(**단일 연결 모드**)**를 비활성화하면 Cisco ISE는 모든 TACACS 요청에 대해 새 TCP 연결을 사용합니다.

SNMP 설정

다음 표에서는 **SNMP Settings(SNMP** 설정**)** 섹션의 필드에 대해 설명합니다.

표 ***4: SNMP*** 설정 영역의 필드

필드 이름	사용 지침
SNMP Version(SNMP 버전**)**	**SNMP Version(SNMP** 버전**)** 드롭다운 목록에서 다음 옵션 중 하나를 선택합니다. • **1**: SNMPv1에서는 알림이 지원되지 않습니다. • **2c** • **3**: SNMPv3은 이후 단계에서 **Priv(**개인**)** 보안 레벨 선택 시 패킷 암호화를 허용하므로 가장 안전한 모델입니다. 참고 SNMPv3 매개변수를 사용하여 네트워크 디바이스를 구성한 경우에는 모니터링 서비스(**Operations(**운영**)** > **Reports(**보고서**)** > **Diagnostics(**진단**)** > **Network Device Session Status(**네트워크 디바이스 세션 상태**))**에서 제공되는 **Network Device Session Status(**네트워크 디바이스 세션 상태**)** 요약 보고서를 생성할 수 없습니다. 네트워크 디바이스가 SNMPv1 또는 SNMPv2c 매개변수로 구성된 경우 이 보고서를 정상적으로 생성할 수 있습니다.
SNMP RO Community(SNMP RO 커뮤니티**)**	(SNMP 버전 1 및 2c에 대해서만 적용됨) 디바이스에 대한 특정 액세스 유형을 Cisco ISE에 제공하는 읽기 전용 커뮤니티 문자열을 입력합니다. 참고 캐럿(circumflex ^) 기호는 허용되지 않습니다.
SNMP Username(SNMP 사용자 이름**)**	(SNMP 버전 3에만 적용됨) SNMP 사용자 이름을 입력합니다.

필드 이름	사용 지침
Security Level(보안 레벨**)**	(SNMP 버전 3에만 적용됨) **Security Level(**보안 레벨**)** 드롭다운 목록에서 다음 옵션 중 하나를 선택합니다. • **Auth(**인증**)**: MD5 또는 SHA(Secure Hash Algorithm) 패킷 인증을 활성화합니다. • **No Auth(**인증 안 함**)**: 인증 및 개인 보안 레벨을 사용하지 않습니다. • **Priv(**개인**)**: DES(Date Encryption Standard, 데이터 암호화 표준) 패킷 암호화를 활성화합니다.
Auth Protocol(인증 프로토콜**)**	(보안 레벨로 **Auth(**인증**)** 또는 **Priv(**개인**)**를 선택하는 경우 SNMP 버전 3에만 적용됨) 네트워크 디바이스가 사용하도록 할 인증 프로토콜을 **Auth Protocol(**인증 프로토콜**)** 드롭다운 목록에서 선택합니다. • **MD5** • **SHA**
Auth Password(인증 비밀번호**)**	(보안 레벨로 **Auth(**인증**)** 및 **Priv(**개인**)**를 선택하는 경우 SNMP 버전 3에만 적용됨) 인증 키를 입력합니다. 8자 이상이어야 합니다. **Show(**표시**)**를 클릭하면 디바이스에 대해 이미 구성된 인증 비밀번호가 표시됩니다. 참고 캐럿(circumflex ^) 기호는 사용할 수 없습니다.
Privacy Protocol(프라이버시 프로토콜**)**	(**Priv(**개인**)** 보안 레벨이 선택된 경우 SNMP 버전 3에만 적용됨) **Privacy Protocol(**프라이버시 프로토콜**)** 드롭다운 목록에서 다음 옵션 중 하나를 선택합니다. • **DES** • **AES128** • **AES192** • **AES256** • **3DES**

필드 이름	사용 지침
Privacy Password(프라이버시 비밀번호**)**	(보안 레벨로 **Priv(**개인**)**를 선택하는 경우 SNMP 버전 3에만 적용됨) 프라이버시 키를 입력합니다. **Show(**표시**)**를 클릭하면 디바이스에 대해 이미 구성된 프라이버시 비밀번호가 표시됩니다. 참고 캐럿(circumflex ^) 기호는 사용할 수 없습니다.
Polling Interval(폴링 간격**)**	폴링 간격을 초 단위로 입력합니다. 기본값은 3600초입니다.
Link Trap Query(링크 트랩 쿼리**)**	SNMP 트랩을 통해 수신되는 linkup 및 linkdown 알림을 수신하고 해석하려면 **Link Trap Query(**링크 트랩 쿼리**)** 확인란을 선택합니다.
Mac Trap Query(Mac 트랩 쿼리**)**	SNMP 트랩을 통해 수신되는 MAC 알림을 수신하고 해석하려면 **Link Trap Query(**링크 트랩 쿼리**)** 확인란을 선택합니다.
Originating Policy Service Node(원래 정책 서비스 노드**)**	**Originating Policy Services Node(**원래 정책 서비스 노드**)** 드롭다운 목록에서 SNMP 데이터 폴링에 사용할 Cisco ISE 서버를 선택합니다. 이 필드의 기본값은 **Auto(**자동**)**입니다. 드롭다운 목록에서 특정 값을 선택하여 설정을 덮어 씁니다.

Advanced TrustSec Settings(Advanced TrustSec 설정)

다음 표에서는 **Advanced TrustSec Settings(**고급 **TrustSec** 설정**)** 섹션의 필드에 대해 설명합니다.

표 ***5:*** 고급 ***TrustSec*** 설정 영역의 필드

필드 이름	사용 지침
Device Authentication Settings(디바이스 인증 설정**)**	
Use Device ID for TrustSec Identification(TrustSec 식별에 디바이스 **ID** 사용**)**	디바이스 이름이 **Device ID(**디바이스 **ID)** 필드에 디바이스 식별자로 나열되도록 하려면 **Use Device ID for TrustSec Identification(TrustSec** 식별에 디바이스 **ID** 사용**)** 확인란을 선택합니다.
Device ID(디바이스 **ID)**	**Use Device ID for TrustSec Identification(TrustSec** 식별에 디바이스 **ID** 사용**)** 확인란을 선택하지 않은 경우에만 이 필드에 디바이스 ID를 입력할 수 있습니다.

필드 이름	사용 지침
Password(비밀번호**)**	Cisco TrustSec 디바이스를 인증하기 위해 Cisco TrustSec 디바이스 CLI에서 구성한 비밀번호를 입력합니다. 비밀번호를 표시하려면 **Show(**표시**)**를 클릭합니다.
HTTP REST API Settings(HTTP REST API 설정**)**	
Enable HTTP REST API(HTTP REST API 활성화**)**	HTTP REST API를 사용하여 필요한 Cisco TrustSec 정보를 네트워크 디바이스에 제공하려면 **Enable HTTP REST API(HTTP REST API** 활성화**)** 확인란을 선택합니다. 이렇게 하면 RADIUS 프로토콜에 비해 짧은 시간에 대규모 구성을 다운로드할 수 있고 효율성이 향상됩니다. 또한 TCP over UDP를 사용하여 안정성이 향상됩니다.
Username(사용자 이름**)**	Cisco TrustSec 디바이스를 인증하기 위해 Cisco TrustSec 디바이스 CLI에서 구성한 사용자 이름을 입력합니다. 사용자 이름에는 특수 문자를 포함할 수 없습니다. 예: 공백 ! % ^ : ; , [{ | }] ` " = < > ?
Password(비밀번호**)**	Cisco TrustSec 디바이스를 인증하기 위해 Cisco TrustSec 디바이스 CLI에서 구성한 비밀번호를 입력합니다.
TrustSec 디바이스 알림 및 업데이트	
Device ID(디바이스 **ID)**	**Use Device ID for TrustSec Identification(TrustSec** 식별에 디바이스 **ID** 사용**)** 확인란을 선택하지 않은 경우에만 이 필드에 디바이스 ID를 입력할 수 있습니다.
Password(비밀번호**)**	Cisco TrustSec 디바이스를 인증하기 위해 Cisco TrustSec 디바이스 CLI에서 구성한 비밀번호를 입력합니다. 비밀번호를 표시하려면 **Show(**표시**)**를 클릭합니다.
Download Environment Data Every <...>(환경 데이터 다운로드 간격**)**	이 영역의 드롭다운 목록에서 필요한 값을 선택하여 디바이스가 Cisco ISE에서 환경 데이터를 다운로드하는 시간 간격을 지정합니다. 초, 분, 시간, 일 또는 주 단위로 시간 간격을 선택할 수 있습니다. 기본값은 1일입니다.

필드 이름	사용 지침
Download Peer Authorization Policy Every <...>(피어 권한 부여 정책 다운로드 간격**)**	이 영역의 드롭다운 목록에서 필요한 값을 선택하여 디바이스가 Cisco ISE에서 피어 권한 부여 정책을 다운로드하는 시간 간격을 지정합니다. 초, 분, 시간, 일 또는 주 단위로 시간 간격을 지정할 수 있습니다. 기본값은 1일입니다.
Reauthentication Every <...>(재인증 간격**)**	이 영역의 드롭다운 목록에서 필요한 값을 선택하여 디바이스가 초기 인증 후 Cisco ISE에 대해 재인증되는 시간 간격을 지정합니다. 초, 분, 시간, 일 또는 주 단위로 시간 간격을 구성할 수 있습니다. 예를 들어 1,000초를 입력하면 디바이스가 Cisco ISE에 대해 1,000초마다 자체적으로 재인증됩니다. 기본값은 1일입니다.
Download SGACL Lists Every <...>(SGACL 목록 다운로드 간격**)**	이 영역의 드롭다운 목록에서 필요한 값을 선택하여 디바이스가 Cisco ISE에서 SGACL 목록을 다운로드하는 시간 간격을 지정합니다. 초, 분, 시간, 일 또는 주 단위로 시간 간격을 구성할 수 있습니다. 기본값은 1일입니다.
Other TrustSec Devices to Trust This Device (TrustSec Trusted)(다른 **TrustSec** 디바이스가 이 디바이스를 신뢰함**(TrustSec** 신뢰**))**	모든 피어 디바이스가 이 Cisco TrustSec 디바이스를 신뢰하도록 허용하려면 **Other TrustSec Devices to Trust This Device(**다른 **TrustSec** 디바이스가 이 디바이스를 신뢰함**)** 확인란을 선택합니다. 이 확인란을 선택하지 않으면 피어 디바이스가 이 디바이스를 신뢰하지 않으며 이 디바이스에서 도착하는 모든 패킷에 그에 따른 색상 또는 태그가 지정됩니다.

필드 이름	사용 지침
구성 변경 사항을 디바이스에 전송	Cisco ISE가 CoA 또는 CLI(SSH)를 사용하여 Cisco TrustSec 디바이스에 Cisco TrustSec 구성 변경 사항을 보내도록 하려면 **Send Configuration Changes to Device(**구성 변경 사항을 디바이스에 전송**)** 확인란을 선택합니다. 필요에 따라 **CoA** 또는 **CLI(SSH)** 라디오 버튼을 클릭합니다. Cisco ISE가 CoA를 사용하여 Cisco TrustSec 디바이스에 구성 변경 사항을 전송하도록 하려면 **CoA** 옵션을 선택합니다. Cisco ISE가 CLI(SSH 연결)를 사용하여 Cisco TrustSec 디바이스에 구성 변경 사항을 전송하도록 하려면 **CLI (SSH)** 옵션을 선택합니다. 자세한 내용은 *Cisco ISE* 관리 가이드*:* 세그멘테이션의 "CoA 미지원 디바이스에 구성 변경 푸시"섹션을 참고하십시오 참고.
Send From(전송 위치**)**	이 드롭다운 목록에서 구성 변경 사항을 Cisco TrustSec 디바이스로 전송할 Cisco ISE 노드를 선택합니다. PAN 또는 PSN 노드를 선택할 수 있습니다. 선택한 PSN 노드가 작동 중지된 경우 PAN을 사용하여 구성 변경 사항이 Cisco TrustSec 디바이스로 전송됩니다.
연결 테스트	이 옵션을 사용하여 Cisco TrustSec 디바이스와 선택한 Cisco ISE 노드(PAN 또는 PSN) 간의 연결을 테스트할 수 있습니다.
SSH Key(SSH 키**)**	이 기능을 사용하려면 Cisco ISE에서 네트워크 디바이스로의 SSHv2 터널을 연 다음 디바이스의 CLI를 사용해 SSH 키를 검색합니다. 검증을 위해 이 키를 복사하여 **SSH Key(SSH** 키**)** 필드에 붙여 넣어야 합니다. 자세한 내용은 *Cisco ISE* 관리 가이드*:* 세그멘테이션의 "SSH 키 확인" 섹션을 참고하십시오.
디바이스 구성 구축	
Include this device when deploying Security Group Tag Mapping Updates(보안 그룹 태그 매핑 업데이트 구축 시 이 디바이스 포함**)**	Cisco TrustSec 디바이스가 디바이스 인터페이스 자격 증명을 사용하여 IP-SGT 매핑을 가져오도록 하려면 **Include this device when deploying Security Group Tag Mapping Updates(**보안 그룹 태그 매핑 업데이트 구축 시 이 디바이스 포함**)** 확인란을 선택합니다.

필드 이름	사용 지침
Exec Mode Username(실행 모드 사용자 이름**)**	Cisco TrustSec 디바이스에 로그인하는 데 사용하는 사용자 이름을 입력합니다.
Exec Mode Password(실행 모드 비밀번호**)**	디바이스 비밀번호를 입력합니다. 비밀번호를 보려면 **Show(**표시**)**를 클릭합니다. 참고 보안 취약점을 방지하려면 EXEC 모드 및 활성화 모드 비밀번호를 포함하여 비밀번호에 % 문자를 사용하지 않는 것이 좋습니다.
Enable Mode Password(활성화 모드 비밀번호**)**	(선택 사항) 특별 권한 모드에서 Cisco TrustSec 디바이스의 구성을 편집하는 데 사용되는 활성화 비밀번호를 입력합니다. 비밀번호를 보려면 **Show(**표시**)**를 클릭합니다.
OOB TrustSec PAC	
Issue Date(발급 날짜**)**	Cisco TrustSec 디바이스에 대해 Cisco ISE에서 마지막으로 생성된 Cisco TrustSec PAC의 발급 날짜를 표시합니다.
만료일	Cisco TrustSec 디바이스에 대해 Cisco ISE에서 마지막으로 생성된 Cisco TrustSec PAC의 만료일을 표시합니다.
Issued By(발급자**)**	Cisco TrustSec 디바이스에 대해 Cisco ISE에서 마지막으로 생성된 Cisco TrustSec PAC의 발급자 이름(Cisco TrustSec 관리자)을 표시합니다.
Generate PAC(PAC 생성**)**	**Generate PAC(PAC** 생성**)** 버튼을 클릭하여 Cisco TrustSec 디바이스에 대한 OOB(Out of Band) Cisco TrustSec PAC를 생성합니다.

기본 네트워크 디바이스 정의 설정

다음 표에서는 **Default Network device(**기본 네트워크 디바이스**)** 창의 필드에 대해 설명합니다. 이 창에서는 Cisco ISE가 RADIUS 또는 TACACS+ 인증에 사용할 수 있는 기본 네트워크 디바이스를 구성할 수 있습니다. 다음 탐색 경로 중 하나를 선택합니다.

- **Administration(**관리**)** > **Network Resources(**네트워크 리소스**)** > **Network Devices(**네트워크 디바이스**)** > **Default Device(**기본 디바이스**)**
- **Work Centers(**작업 센터**)** > **Device Administration(**디바이스 관리**)** > **Network Resources(**네트워크 리소스**)** > **Default Devices(**기본 디바이스**)**

표 ***6: Default Network Device(***기본 네트워크 디바이스***)*** 창의 필드

필드 이름	사용 지침
Default Network Device Status(기본 네트워크 디바이스 상태**)**	**Default Network Device Status(**기본 네트워크 디바이스 상태**)** 드롭다운 목록에서 **Enable(**활성화**)**를 선택하여 기본 네트워크 디바이스 정의를 활성화합니다. 참고 기본 디바이스를 활성화하는 경우 이 창에서 RADIUS 또는 TACACS+ 인증 설정의 해당 확인란을 선택하여 활성화해야 합니다.
디바이스 프로파일**(Device Profile)**	**Cisco**를 기본 디바이스 벤더로 표시합니다.
RADIUS 인증 설정**(RADIUS Authentication Settings)**	
Enable RADIUS(RADIUS 활성화**)**	디바이스에 대한 RADIUS 인증을 활성화하려면 **Enable RADIUS(RADIUS** 활성화**)** 확인란을 선택합니다.
RADIUS UDP 설정**(RADIUS UDP Settings)**	
Shared Secret(공유 암호**)**	공유 암호를 입력합니다. 공유 암호의 최대 길이는 127자입니다. 공유 암호는 **radius-host** 명령(**pac** 옵션 포함)을 사용하여 네트워크 디바이스에서 구성한 키입니다. 참고 공유 암호 길이는 **Device Security Settings(**디바이스 보안 설정**)** 창(**Administration(**관리**)** > **Network Resources(**네트워크 리소스**)** > **Network Devices(**네트워크 디바이스**)** > **Device Security Settings(**네트워크 보안 설정**))** 창의 **Minimum RADIUS Shared Secret Length(**최소 **RADIUS** 공유 암호 길이**)** 필드에 구성된 값보다 크거나 같아야 합니다. 기본적으로 이 값은 신규 설치 및 업그레이드된 구축의 경우 4자입니다. RADIUS 서버의 경우 모범 사례는 22자입니다.
RADIUS DTLS Settings(RADIUS DTLS 설정**)**	

필드 이름	사용 지침
DTLS Required(DTLS 필수**)**	**DTLS Required(DLTS** 필수**)** 확인란을 선택하면 Cisco ISE에서 이 디바이스의 DTLS 요청만 처리합니다. 이 옵션을 비활성화하면 Cisco ISE에서 이 디바이스의 UDP 요청과 DTLS 요청을 모두 처리합니다. RADIUS DTLS는 SSL 터널 설정 및 RADIUS 통신을 위한 향상된 보안을 제공합니다.
Shared Secret(공유 암호**)**	RADIUS DTLS에 사용되는 공유 암호를 표시합니다. 이 값은 고정되어 있으며 MD5 무결성 확인을 컴퓨팅하는 데 사용됩니다.
Issuer CA of ISE Certificates for CoA(CoA의 **ISE** 인증서에 대한 발급자 **CA)**	**Issuer CA of ISE Certificates for CoA(CoA**의 **ISE** 인증서에 대한 발급자 **CA)** 드롭다운 목록에서 RADIUS DTLS CoA에 사용할 인증 기관을 선택합니다.
General Settings(일반 설정**)**	
Enable KeyWrap(KeyWrap 활성화**)**	네트워크 디바이스에서 KeyWrap 알고리즘이 지원되는 경우에만 **Enable KeyWrap(KeyWrap** 활성화**)** 확인란을 선택합니다. 확인란을 선택하면 AES KeyWrap 알고리즘을 통해 RADIUS 보안이 개선됩니다.
Key Encryption Key(키 암호화 키**)**	KeyWrap을 활성화하는 경우 세션 암호화(비밀 유지)에 사용할 암호화 키를 입력합니다.
Message Authenticator Code Key(메시지 인증자 코드 키**)**	KeyWrap을 활성화하는 경우 RADIUS 메시지에 대한 키 HMAC(Hashed Message Authentication Code) 계산에 사용되는 키를 입력합니다.
Key Input Format(키 입력 형식**)**	다음 형식 중 하나의 해당 라디오 버튼을 클릭하여 선택하고 **Key Encryption Key(**키 암호화 키**)** 및 **Message Authenticator Code Key(**메시지 인증자 코드 키**)** 필드에 값을 입력합니다. • **ASCII**: 키 암호화 키의 길이는 16자(바이트)여야 하며 메시지 인증자 코드 키의 길이는 20자(바이트)여야 합니다. • **Hexadecimal(16**진수**)**: 키 암호화 키의 길이는 32바이트여야 하며 메시지 인증자 코드 키의 길이는 40바이트여야 합니다.
TACACS Authentication Settings(TACACS 인증 설정**)**	

필드 이름	사용 지침
Shared Secret(공유 암호**)**	TACACS+ 프로토콜을 활성화할 때 네트워크 디바이스에 할당된 텍스트 문자열입니다. 네트워크 디바이스가 사용자 이름과 비밀번호를 인증하기 전에 사용자가 텍스트를 입력해야 합니다. 사용자가 공유 암호를 제공할 때까지는 연결이 거부됩니다.
Retired Shared Secret is Active(사용 중단된 공유 암호가 활성 상태임**)**	사용 중단 기간이 활성인 경우 표시됩니다.
Retire(사용 중단**)**	기존 공유 암호를 종료하는 대신 사용 중단합니다. **Retire(**사용 중단**)**를 클릭하면 메시지 상자가 표시됩니다. **Yes(**예**)** 또는 **No(**아니요**)**를 클릭합니다.
Remaining Retired Period(남은 사용 중단 기간**)**	(위의 메시지 상자에서 **Yes(**예**)**를 선택한 경우에만 사용 가능함) **Work Centers(**작업 센터**)** > **Device Administration(**디바이스 관리**)** > **Settings(**설정**)** > **Connection Settings(**연결 설정**)** > **Default Shared Secret Retirement Period(**기본 공유 암호 사용 중단 기간**)** 탐색 경로에 지정되어 있는 기본값이 표시됩니다. 기본값은 변경할 수 있습니다. 그러면 새 공유 암호를 입력할 수 있으며, 이전 공유 암호는 지정된 기간(일) 동안 활성 상태로 유지됩니다.
End(종료**)**	(위의 메시지 상자에서 **Yes(**예**)**를 선택한 경우에만 사용 가능함) 사용 중단 기간을 종료하고 이전 공유 암호 사용을 중단합니다.
Enable Single Connect Mode(단일 연결 모드 활성화**)**	네트워크 디바이스와의 모든 TACACS+ 통신에 단일 TCP 연결을 사용하려면 **Enable Single Connect Mode(**단일 연결 모드 활성화**)** 확인란을 선택합니다. 다음 중 하나의 옵션에 해당하는 라디오 버튼을 클릭합니다. • **Legacy Cisco Devices(**레거시 **Cisco** 디바이스**)** • **TACACS Draft Compliance Single Connect Support(TACACS+** 초안 규정 준수 단일 연결 지원**)**. 이 옵션을 비활성화하면 Cisco ISE는 모든 TACACS+ 요청에 대해 새 TCP 연결을 사용합니다.

네트워크 디바이스 가져오기 설정

다음 표에서는 Cisco ISE로 네트워크 디바이스 세부정보를 가져오는 데 사용할 수 있는 네트워크 디바이스 가져오기 페이지의 필드에 대해 설명합니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Network Resources(**네트워크 리소스**)** > **Network Devices(**네트워크 디바이스**)** 입니다.

표 *7:* 네트워크 디바이스 가져오기 설정

필드 이름	사용 지침
Generate a Template(템플릿 생성**)**	쉼표로 구분된 값(CSV) 템플릿 파일을 생성하려면 **Generate a Template(**템플릿 생성**)**을 클릭합니다. 동일한 형식의 네트워크 디바이스 정보로 템플릿을 업데이트하고 로컬에 저장합니다. 그런 다음 편집된 템플릿을 사용하여 네트워크 디바이스를 Cisco ISE 구축으로 가져옵니다.
파일	**Choose File(**파일 선택**)**을 클릭하여, 최근에 직접 생성했거나 이전에 Cisco ISE 구축에서 내보냈을 수 있는 CSV 파일을 선택합니다. **Import(**가져오기**)** 옵션을 사용하면 신규/업데이트된 네트워크 디바이스 정보가 포함된 다른 Cisco ISE 구축의 네트워크 디바이스를 가져올 수 있습니다.
Overwrite Existing Data with New Data(새 데이터로 기존 데이터 덮어쓰기**)**	Cisco ISE가 기존 네트워크 디바이스를 가져오기 파일의 디바이스로 교체하도록 하려면 **Overwrite Existing Data with New Data(**새 데이터로 기존 데이터 덮어쓰기**)** 확인란을 선택합니다. 이 확인란을 선택하지 않으면 가져오기 파일에서 사용 가능한 새 네트워크 디바이스 정의가 네트워크 디바이스 저장소에 추가됩니다. 중복 엔트리는 무시됩니다.
Stop Import on First Error(첫 번째 오류에서 가져오기 중지**)**	가져오기 중에 오류가 발생하는 경우 Cisco ISE가 가져오기를 중단하게 하려면 **Stop Import on First Error(**첫 번째 오류에서 가져오기 중지**)** 확인란을 선택합니다. 그러면 Cisco ISE는 오류가 발생할 때까지 네트워크 디바이스를 가져옵니다. 이 확인란을 선택하지 않은 상태에서 발생하는 오류는 보고되며 Cisco ISE는 나머지 디바이스 가져오기를 계속합니다.

Cisco ISE에서 네트워크 디바이스 추가

Cisco ISE에서 네트워크 디바이스를 추가하거나 기본 네트워크 디바이스를 사용할 수 있습니다.

Network Devices(네트워크 디바이스**)**(**Work Centers(**작업 센터**)** > **Device Administration(**디바이스 관리**)** > **Network Resources(**네트워크 리소스**)** > **Network Devices(**네트워크 디바이스**)**) 창에서 네트워크 디바이스를 추가할 수도 있습니다.

시작하기 전에

추가할 네트워크 디바이스에서 AAA 기능을 활성화해야 합니다. 릴리스에 대한 *Cisco ISE* 관리자 가이드의 "통합" 장에서 "AAA 기능을 활성화하는 명령" 섹션을 참조하십시오.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Network Resources(**네트워크 리소스**)** > **Network Devices(**네트워크 디바이스**)**를 선택합니다.

단계 **2** **Add(**추가**)**를 클릭합니다.

단계 **3** **Name(**이름**)**, **Description(**설명**)** 및 **IP Address(IP** 주소**)** 필드에 해당 값을 입력합니다.

단계 **4** 드롭다운 목록에서 **Device Profile(**디바이스 프로파일**)**, **Model Name(**모델 이름**)**, **Software Version(**소프트웨어 버전**)** 및 **Network Device Group(**네트워크 디바이스 그룹**)** 필드에 필요한 값을 선택합니다.

단계 **5** (선택 사항) 인증용 RADIUS 프로토콜을 구성하려면 **RADIUS Authentication Settings(RADIUS** 인증 설정**)** 확인란을 선택합니다.

단계 **6** (선택 사항) 인증용 TACACS 프로토콜을 구성하려면 **TACACS Authentication Settings(TACACS** 인증 설정**)** 확인란을 선택합니다.

단계 **7** (선택 사항) 네트워크 디바이스에서 정보를 수집하기 위해 Cisco ISE 프로파일링 서비스용으로 SNMP를 구성하려면 **SNMP Settings(SNMP** 설정**)** 확인란을 선택합니다.

단계 **8** (선택 사항) Cisco TrustSec이 활성화된 디바이스를 구성하려면 **Advanced TrustSec Settings(**고급 **TrustSec** 설정**)** 확인란을 선택합니다.

단계 **9** **Submit(**제출**)**을 클릭합니다.

Cisco ISE로 네트워크 디바이스 가져오기

Cisco ISE가 네트워크 디바이스와 통신하도록 하려면 Cisco ISE에서 네트워크 디바이스의 디바이스 정의를 추가해야 합니다. **Network Devices(**네트워크 디바이스**)** 창(메인 메뉴에서 **Administration(**관리**)** > **Network Resources(**네트워크 리소스**)** > **Network Devices(**네트워크 디바이스**)**)을 통해 Cisco ISE로 네트워크 디바이스의 디바이스 정의를 가져옵니다.

CSV(comma-separated value) 파일을 사용하여 Cisco ISE 노드로 디바이스 정의 목록을 가져옵니다. **Network Devices(**네트워크 디바이스**)** 창에서 **Import(**가져오기**)**를 클릭하면 CSV 템플릿 파일을 사용할 수 있습니다. 해당 파일을 다운로드하고 원하는 디바이스 정의를 입력한 다음, **Import(**가져오기**)** 창을 통해 편집한 파일을 업로드합니다.

같은 리소스 유형의 가져오기를 동시에 여러 개 실행할 수는 없습니다. 예를 들어 서로 다른 두 가져오기 파일에서 네트워크 디바이스를 동시에 가져올 수는 없습니다.

디바이스 정의의 CSV 파일을 가져올 때 **Overwrite Existing Data with New Data(**새 데이터로 기존 데이터 덮어쓰기**)** 옵션을 클릭하여 새 기록을 생성하거나 기존 기록을 업데이트할 수 있습니다.

가져오기 템플릿은 Cisco ISE마다 다를 수 있습니다. 다른 Cisco ISE 릴리스에서 내보낸 네트워크 디바이스의 CSV 파일을 가져오지 마십시오. 릴리스의 CSV 템플릿 파일에 네트워크 디바이스의 세부 정보를 입력하고 해당 파일을 Cisco ISE로 가져옵니다.

참고 모든 octet의 IP 범위가 있는 네트워크 디바이스를 가져올 수 있습니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Network Resources(**네트워크 리소스**)** > **Network Devices(**네트워크 디바이스**)**를 선택합니다.

단계 **2** **Import(**가져오기**)**를 클릭합니다.

단계 **3** 표시되는 **Import Network Devices(**네트워크 디바이스 가져오기**)** 창에서 **Generate A Template(**템플릿 생성**)**을 클릭하여 CSV 파일을 다운로드합니다. 이 파일을 편집해서 필요한 세부정보를 포함하여 Cisco ISE로 가져올 수 있습니다.

단계 **4** **Choose File(**파일 선택**)**을 클릭하여 클라이언트 브라우저를 실행 중인 시스템에서 CSV 파일을 선택합니다.

단계 **5** (선택 사항) 필요에 따라 **Overwrite Existing Data with New Data(**새 데이터로 기존 데이터 덮어쓰기**)** 및 **Stop Import on First Error(**첫 번째 오류에서 가져오기 중지**)** 확인란을 선택합니다.

단계 **6** **Import(**가져오기**)**를 클릭합니다.

파일을 모두 가져오면 Cisco ISE에 요약 메시지가 표시됩니다. 요약 메시지에는 가져오기 상태(성공 또는 실패), 발생한 오류 수(있는 경우), 파일 가져오기 프로세스에 소요된 총 처리 시간이 포함됩니다.

Cisco ISE에서 네트워크 디바이스 내보내기

Cisco ISE 노드에서 사용 가능한 네트워크 디바이스의 디바이스 정의를 CSV 파일 형식으로 내보낼 수 있습니다. 그런 다음 필요한 Cisco ISE 노드에서 디바이스 정의를 사용할 수 있도록 이 CSV 파일을 다른 Cisco ISE 노드로 가져올 수 있습니다.

참고 모든 octet의 IP 범위가 있는 네트워크 디바이스를 내보낼 수 있습니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Network Resources(**네트워크 리소스**)** > **Network Devices(**네트워크 디바이스**)**를 선택합니다.

단계 **2** **Export(**내보내기**)**를 클릭합니다.

단계 **3** 다음 작업 중 하나를 수행하여 Cisco ISE 노드에 추가된 네트워크 디바이스에 대한 디바이스 정의를 내보냅니다.

- 내보낼 디바이스 옆의 확인란을 선택하고 **Export(**내보내기**)**를 클릭하여 드롭다운 목록에서 **Export Selected(**선택 항목 내보내기**)**를 선택합니다.

- **Export(**내보내기**)**를 클릭하고 드롭다운 목록에서 **Export All(**모두 내보내기**)**을 선택하여 Cisco ISE 노드에 추가된 모든 네트워크 디바이스를 내보냅니다.

단계 **4** 두 경우 모두 디바이스 정의에 대한 CSV 파일이 시스템에 다운로드됩니다.

네트워크 디바이스 컨피그레이션 문제 해결

단계 **1** Cisco ISE GUI에서 **Menu(**메뉴**)** 아이콘(☰)을 클릭하고**Operations(**운영**)** > **Troubleshoot(**문제 해결**)** > **Diagnostic Tools(**진단 도구**)** > **General Tools(**일반 도구**)** > **Evaluate Configuration Validator(**구성 검증기 평가**)**를 선택합니다.

단계 **2** 구성을 평가할 네트워크 디바이스의 IP 주소를 **Network Device IP(**네트워크 디바이스 **IP)** 필드에 입력합니다.

단계 **3** 확인란을 선택하고 권장 템플릿과 비교할 구성 옵션 옆의 라디오 버튼을 클릭합니다.

단계 **4** **Run(**실행**)**을 클릭합니다.

단계 **5** 표시되는 **Progress Details...(**진행 세부정보**)** 영역에서 **Click Here to Enter Credentials(**여기를 클릭하여 자격 증명 입력**)**를 클릭합니다. **Credentials Window(**자격 증명 창**)** 대화 상자에서 네트워크 디바이스와의 연결을 설정하는 데 필요한 연결 매개변수 및 자격 증명을 입력하고 **Submit(**제출**)**를 클릭합니다

워크플로우를 취소하려면 **Progress Details...(**진행 세부정보...**)** 창에서 **Click Here to Cancel the Running Workflow(**여기를 클릭하여 실행 중인 워크플로우 취소**)**를 클릭합니다.

단계 **6** 분석할 인터페이스 옆의 확인란을 선택하고 **Submit(**제출**)**을 클릭합니다.

단계 **7** 구성 평가에 대한 자세한 내용을 보려면 **Show Results Summary(**결과 요약 표시**)**를 클릭합니다.

네트워크 디바이스 명령 진단 도구 실행

네트워크 디바이스 실행 명령 진단 도구를 사용하면 네트워크 디바이스에 대해 **show** 명령을 실행할 수 있습니다.

표시되는 결과는 콘솔에 표시되는 것과 동일합니다. 이 도구를 사용하면 디바이스 컨피그레이션의 모든 문제를 식별할 수 있습니다.

네트워크 디바이스의 컨피그레이션을 확인하거나 네트워크 디바이스가 구성된 방법을 확인하려면 이 도구를 활용하면 됩니다.

네트워크 디바이스 실행 명령 진단 도구에 액세스하려면 다음 탐색 경로 중 하나를 선택하십시오.

- Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고**Operations(**운영**)** > **Troubleshoot(**문제 해결**)** > **Diagnostic Tools(**진단 도구**)** > **Execute Network Device Command(**네트워크 디바이스 명령 실행**)**를 선택합니다.
- Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고**Work Centers(**작업 센터**)** > **Profiler(**프로파일러**)** > **Troubleshoot(**문제 해결**)** > **Execute Network Device Command(**네트워크 디바이스 명령 실행**)**를 선택합니다.

표시되는 **Execute Network Device Command(**네트워크 디바이스 실행 명령**)** 창에서 해당 필드에 실행할 네트워크 디바이스의 IP 주소와 show 명령을 입력합니다. **Run(**실행**)**을 클릭합니다.

Cisco ISE의 서드파티 네트워크 디바이스 지원

Cisco ISE는 네트워크 디바이스 프로파일을 사용하여 서드파티 NAD(Network Access Device)를 지원합니다. NAD 프로파일은 벤더 쪽 구현에 관계없이 간소화된 정책 컨피그레이션을 사용하여 서드파티 디바이스 기능을 정의합니다. 네트워크 디바이스 프로파일에는 다음이 포함됩니다.

- RADIUS, TACACS+, Cisco TrustSec 등 네트워크 디바이스가 지원하는 프로토콜. 네트워크 디바이스용으로 존재하는 벤더별 RADIUS 사전을 Cisco ISE로 가져올 수 있습니다.
- 디바이스가 유선 MAB 및 802.1X 등의 다양한 인증 플로우에 사용하는 속성과 값. Cisco ISE는 이러한 속성 및 값을 사용하여, 네트워크 디바이스가 사용하는 속성에 따라 디바이스에 적합한 인증 플로우를 탐지할 수 있습니다.
- 네트워크 디바이스에 있는 CoA(Change of Authorization) 기능. RADIUS 프로토콜 RFC 5176은 CoA 요청을 정의하지만 CoA 요청에 사용되는 속성은 네트워크 디바이스에 따라 달라집니다. RFC 5176을 지원하는 대부분의 Cisco 이외의 디바이스는 "푸시" 및 "연결 끊기" 기능을 지원합니다. RADIUS CoA 유형을 지원하지 않는 디바이스의 경우 Cisco ISE는 SNMP CoA도 지원합니다.
- 네트워크 디바이스가 MAB 플로우에 사용하는 속성 및 프로토콜. 여러 벤더의 네트워크 디바이스는 각기 다른 방식으로 MAB 인증을 수행합니다.
- 디바이스에서 사용하는 VLAN 및 ACL 권한. 프로파일을 저장하면 Cisco ISE는 구성된 각 권한에 대해 권한 부여 프로파일을 자동으로 생성합니다.
- URL 리디렉션 기술 정보. BYOD(Bring Your Own Device), 게스트 액세스, 포스처 서비스 등의 고급 플로우에서는 URL 리디렉션이 필요합니다. 네트워크 디바이스에서는 두 가지 유형의 URL 리디렉션(정적 및 동적)을 확인할 수 있습니다. 정적 URL 리디렉션의 경우 Cisco ISE 포털 URL을 복사하여 컨피그레이션에 붙여 넣을 수 있습니다. 동적 URL 리디렉션의 경우 Cisco ISE는 RADIUS 속성을 사용하여 리디렉션 대상 위치를 네트워크 디바이스에 알려 줍니다.

  디바이스가 동적 및 정적 URL 리디렉션을 모두 지원하지 않는 경우 Cisco ISE는 URL 리디렉션 시뮬레이션에 사용하는 인증 VLAN 컨피그레이션을 제공합니다. 인증 VLAN 컨피그레이션은 Cisco ISE에서 실행되는 DHCP 및 DNS 서비스를 기반으로 합니다.

Cisco ISE에서 네트워크 디바이스를 정의한 후 프로파일러, 게스트, BYOD, MAP, 보안 상태 등 고급 플로우와 함께 기본 인증 플로우를 활성화하는 데 사용하는 기능을 정의하기 위해 이러한 디바이스 프로파일을 구성하거나 Cisco ISE에서 제공하는 사전 구성된 디바이스 프로파일을 사용합니다.

URL 리디렉션 메커니즘 및 인증 VLAN

네트워크에서 서드파티 디바이스를 사용하며 해당 디바이스가 동적 또는 정적 URL 리디렉션을 지원하지 않는 경우, ISE는 URL 리디렉션 플로우를 시뮬레이션합니다. 이러한 디바이스에 대한 URL 리디렉션 시뮬레이션 플로우는 Cisco ISE에서 DHCP 또는 DNS 서비스를 실행하여 작동합니다.

다음은 인증 VLAN 플로우의 예입니다.

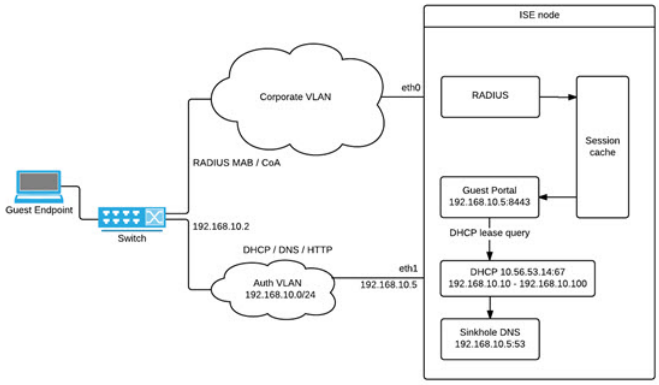
1. 게스트 엔드포인트가 NAD에 연결됩니다.
2. 네트워크 디바이스가 RADIUS 또는 MAB 요청을 Cisco ISE에 보냅니다.
3. ISE가 구성된 인증 및 권한 부여 정책을 실행하고 사용자 계정 관리 정보를 저장합니다.
4. ISE가 인증 VLAN ID를 포함하는 RADIUS 액세스-수락 메시지를 보냅니다.
5. 게스트 엔드포인트가 네트워크 액세스 권한을 수신합니다.
6. 엔드포인트가 DHCP 요청을 브로드캐스트하고 Cisco ISE DHCP 서비스에서 클라이언트 IP 주소 및 Cisco ISE DNS 싱크홀 IP 주소를 가져옵니다.
7. 게스트 엔드포인트에서 브라우저를 열고 여기에서 DNS 쿼리를 전송하고 Cisco ISE IP 주소를 수신합니다.
8. 엔드포인트 HTTP 및 HTTPS 요청이 Cisco ISE로 전송됩니다.
9. Cisco ISE가 게스트 포털 URL이 있는 HTTP 301 Moved 메시지로 응답합니다. 엔드포인트 브라우저가 게스트 포털 창으로 리디렉션됩니다.
10. 게스트 엔드포인트 사용자가 인증을 위해 로그인합니다.
11. Cisco ISE가 엔드포인트 규정 준수를 확인한 다음 NAD에 응답합니다. Cisco ISE가 CoA를 전송하고 엔드포인트에 권한을 부여하며 싱크홀을 우회합니다.
12. 게스트 사용자는 CoA를 기준으로 적절한 액세스 권한을 부여받습니다. 엔드포인트는 엔터프라이즈 DHCP에서 IP 주소를 수신합니다. 이제 게스트 사용자가 네트워크를 사용할 수 있습니다.

엔드포인트가 인증을 통과하기 전에 게스트 엔드포인트가 무단으로 네트워크에 액세스할 수 없도록 하기 위해 기업 네트워크에서 인증 VLAN을 분리할 수 있습니다. Cisco ISE 머신을 가리키도록 인증 VLAN IP 헬퍼를 구성하거나 Cisco ISE 네트워크 인터페이스 중 하나를 인증 VLAN에 연결합니다.

NAD 컨피그레이션에서 VLAN IP 헬퍼를 구성하여 여러 VLAN을 하나의 네트워크 인터페이스 카드에 연결할 수 있습니다. IP 헬퍼 구성에 대한 자세한 내용은 네트워크 디바이스의 관리 설명서에서 지침을 참고하십시오. IP 헬퍼가 있는 VLAN을 포함하는 게스트 액세스 플로우의 경우, 게스트 포털을 정의하고 MAB 권한 부여에 바인딩된 권한 부여 프로파일에서 해당 포털을 선택합니다. 게스트 포털에 관한 자세한 정보는 *Cisco ISE* 관리 가이드*:* 게스트 및 *BYOD*에서 Cisco ISE 게스트 서비스 섹션을 참조하십시오. 참고.

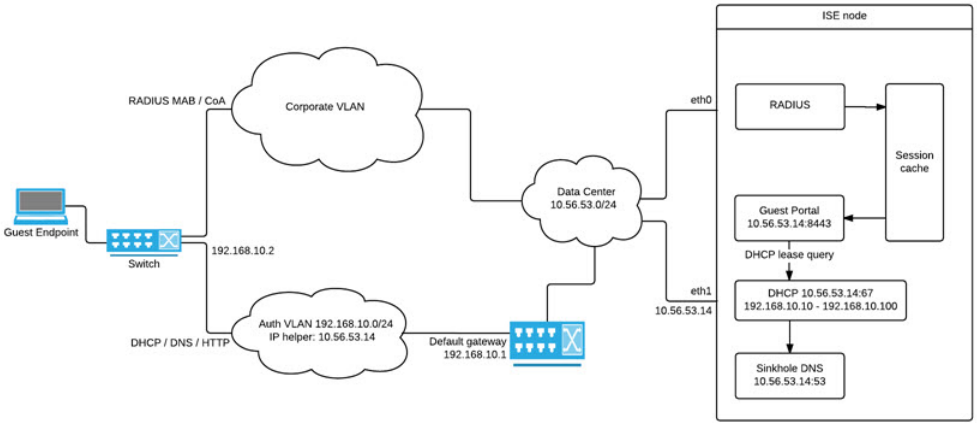
다음 다이어그램에는 인증 VLAN을 정의할 때의 기본 네트워크 설정이 나와 있습니다(인증 VLAN은 Cisco ISE 노드에 직접 연결됨).

그림 *1: Cisco ISE* 노드에 연결되는 인증 *VLAN*



다음 다이어그램에는 인증 VLAN 및 IP 헬퍼가 있는 네트워크가 나와 있습니다.

그림 *2: IP* 헬퍼를 이용해 구성된 인증 *VLAN*



CoA 유형

Cisco ISE는 RADIUS 및 SNMP CoA 유형을 모두 지원합니다. 복잡한 플로우에서 NAD가 작동하려면 RADIUS 또는 SNMP CoA 유형이 지원되어야 하지만 기본 플로우의 경우에는 이러한 유형이 반드시 지원되지 않아도 됩니다.

Cisco ISE에서 NAD를 구성할 때 네트워크 디바이스에서 지원하는 RADIUS 및 SNMP 설정을 정의하고, NAD 프로파일을 구성할 때 특정 플로우에 대해 사용할 CoA 유형을 나타냅니다. NAD용 프로토콜을 정의하는 방법에 대한 자세한 내용은 네트워크 디바이스 정의 설정, 3 페이지를 참고하십시오. Cisco ISE에서 디바이스 및 NAD 프로파일을 생성하기 전에 서드파티 공급업체에 문의하여 NAD가 지원하는 유형을 확인하십시오.

네트워크 디바이스 프로파일

Cisco ISE는 네트워크 디바이스 프로파일을 사용하여 일부 타사 NAD(Network Access Device)를 지원합니다. 이러한 프로파일은 Cisco ISE가 기본 플로우 및 게스트, BYOD, MAB, 포스처 등의 고급 플로우를 활성화하는 데 사용하는 기능을 정의합니다.

Cisco ISE에는 여러 벤더의 네트워크 디바이스용으로 사전 정의된 프로파일이 포함되어 있습니다. Cisco ISE 2.1 이상 릴리스는 다음 표에 나열된 네트워크 디바이스와 함께 테스트되었습니다.

표 ***8: Cisco ISE 2.1*** 이상 릴리즈에서 테스트한 벤더 디바이스

디바이스 유형	벤더	**CoA** 유형	**URL** 리디렉션 유형	지원 및 검증된 활용 사례				
				802.1X 및 **MAB** 플로우	**CoA**가 없는 프로파일러	**CoA**가 있는 프로파일러	포스처	게스트 및 **BYOD** 플로우
무선	Aruba 7000, InstantAP	RADIUS	정적 URL	예	예	예	예	예
	Motorola RFS 4000	RADIUS	동적 URL	예	예	예	예	예
	HP 830	RADIUS	정적 URL	예	예	예	예	예
	Ruckus ZD 1200	RADIUS	—	예	예	예	예	예
유선	HP A5500	RADIUS	ISE에서 제공하는 인증 VLAN	예	예	예	예	예
	HP 3800 및 2920(ProCurve)	RADIUS	ISE에서 제공하는 인증 VLAN	예	예	예	예	예
	Alcatel 6850	SNMP	동적 URL	예	예	예	예	예
	Brocade ICX 6610	RADIUS	ISE에서 제공하는 인증 VLAN	예	예	예	예	예
	Juniper EX3300-24p	RADIUS	ISE에서 제공하는 인증 VLAN	예	예	예	예	예

기타 타사 NAD의 경우 디바이스 속성과 기능을 식별하고 Cisco ISE에서 맞춤형 NAD 프로파일을 생성해야 합니다.	예	예	CoA 지원 필요	CoA 지원이 필요합니다. 유선 디바이스가 URL 리디렉션을 지원하지 않는 경우 Cisco ISE는 인증 VLAN을 사용합니다. 무선 디바이스는 인증 VLAN을 사용하여 테스트되지 않았습니다.

미리 정의된 프로파일이 없는 기타 타사 네트워크 디바이스의 경우 맞춤형 NAD 프로파일을 생성해야 합니다. 게스트, BYOD 및 포스처와 같은 고급 플로우의 경우 네트워크 디바이스가 CoA 이러한 플로우에 대한 지원은 NAD 기능에 따라 달라집니다. Cisco ISE에서 네트워크 디바이스 프로파일을 생성하는 데 필요한 속성에 자세한 내용은 디바이스 관리 가이드를 참조하십시오.

Cisco ISE 릴리스 2.0 이하에서 Cisco ISE 릴리스 2.1 이상으로 업그레이드하는 경우 이전 릴리스에서 비 Cisco NAD와 통신하기 위해 생성한 인증 정책 규칙 및 RADIUS 사전은 업그레이드 후에도 Cisco ISE에서 계속 작동합니다.

ISE Community Resource(ISE 커뮤니티 리소스)

타사 NAD 프로파일에 자세한 내용은 ISE 타사 NAD 프로파일 및 컨피그레이션을 참조하십시오.

Cisco ISE에서 서드파티 네트워크 디바이스 구성

Cisco ISE는 네트워크 디바이스 프로파일을 사용하여 서드 파티 NAD를 지원합니다. 이러한 프로파일은 Cisco ISE가 게스트, BYOD, MAB, 포스처 등의 플로우를 활성화하는 데 사용하는 기능을 정의합니다.

시작하기 전에

네트워크 디바이스 프로파일, 29 페이지의 내용을 참조하십시오.

단계 **1** Cisco ISE에서 서드파티 네트워크 디바이스 추가(Cisco ISE로 네트워크 디바이스 가져오기, 23 페이지 참고) 게스트, BYOD 또는 포스처 워크플로우를 구성하는 경우 CoA(Change of Authorization)가 정의되어 있으며 NAD의 URL 리디렉션 메커니즘이 관련 Cisco ISE 포털을 가리키도록 구성되어 있는지 확인합니다. URL 리디렉션을 구성하려면 포털의 랜딩 페이지에서 Cisco ISE 포털 URL을 복사합니다. Cisco ISE에서 NAD에 대한 CoA 유형 및 URL 리디렉션 구성에 대한 자세한 내용은 네트워크 디바이스 정의 설정, 3 페이지를 참고하십시오. 또한 서드파티 디바이스의 관리 설명서에 나와 있는 지침을 참고하십시오.

단계 **2** 디바이스용으로 적절한 NAD 프로파일을 ISE에서 사용할 수 있는지 확인합니다. 기존 프로파일을 확인하려면 **Administration(**관리**)** > **Network Resources(**네트워크 리소스**)** > **Network Device Profiles(**네트워크 디바이스 프로파일**)**를 선택합니다. Cisco ISE에 적절한 프로파일이 아직 없으면 사용자 맞춤화 프로파일을 생성합니다. 맞춤형 프로파일을 생성하는 방법에 대한 자세한 내용은 네트워크 디바이스 프로파일 생성, 31 페이지을 참고하십시오.

단계 **3** 구성하려는 NAD에 NAD 프로파일을 할당합니다. Cisco ISE GUI에서 **Menu(**메뉴**)** 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Network Resources(**네트워크 리소스**)** > **Network Devices(**네트워크 디바이스**)**. 프로파일을 할당할 디바이스를 열고 **Device Profile(**디바이스 프로파일**)**의 드롭다운 목록에서 올바른 프로파일을 선택합니다.

단계 **4** 정책 규칙을 구성할 때 VLAN 또는 ACL만 사용하거나 네트워크에 여러 벤더의 각기 다른 디바이스가 있는 경우 권한 부여 프로파일을 1단계에서 NAD 프로파일 또는 "Any(모두)"로 명시적으로 설정해야 합니다. 권한 부여 프로파일에 대해 NAD 프로파일을 설정하려면 **Policy(**정책**)** > **Policy Elements(**정책 요소**)** > **Results(**결과**)** > **Authorization(**권한 부여**)** > **Authorization Profiles(**권한 부여 프로파일**)**를 선택합니다. 관련 권한 부여 프로파일을 열고 **Network Device Profile(**네트워크 디바이스 프로파일**)**의 드롭다운 목록에서 관련 NAD 프로파일을 선택합니다. 또한 게스트 플로우에 대해 인증 VLAN을 사용하는 경우 게스트 포털을 정의한 다음 일반 게스트 플로우와 비슷하게 MAB 권한 부여로 바인딩되는 권한 부여 프로파일에서 해당 포털을 선택해야 합니다. 게스트 포털에 관한 자세한 내용은 *Cisco ISE* 관리 가이드*:* 게스트 및 *BYOD*에서 Cisco ISE 게스트 서비스 섹션을 참고하십시오. 참고.

네트워크 디바이스 프로파일 생성

시작하기 전에

- 대부분의 NAD에는 표준 IETF RADIUS 속성 외에 다수의 벤더별 속성을 제공하는 벤더별 RADIUS 사전이 있습니다. 네트워크 디바이스에 벤더별 RADIUS 사전이 있으면 Cisco ISE로 가져옵니다. RADIUS 사전이 필요한 지침은 서드파티 디바이스의 관리 설명서를 참고하십시오. Cisco ISE GUI에서 **Menu(**메뉴**)** 아이콘을 클릭하고(☰) **Policy(**정책**)** > **Policy Elements(**정책 요소**)** > **Dictionaries(**사전**)** > **System(**시스템**)** > **Radius(RADIUS)** > **RADIUS Vendors(RADIUS** 벤더**)**를 선택합니다. RADIUS 사전을 가져오려면 Cisco ISE Admin Guide: Secure Wired Access의 *"RADIUS-*벤더 사전 생성*"* 항목을 확인하십시오. .
- 게스트 및 포스처와 같은 복잡한 플로우의 경우 네트워크 디바이스는 RFC 5176을 지원해야합니다.
- 네트워크 디바이스 프로파일을 생성하기 위한 필드 및 가능한 값에 대한 자세한 내용은 Cisco ISE 관리 가이드: 보안 유선 액세스의 네트워크 디바이스 프로파일 설정 섹션을 참조하십시오. .

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Network Resources(**네트워크 리소스**)** > **Network Device Profiles(**네트워크 디바이스 프로파일**)**를 선택합니다.

단계 **2** **Add(**추가**)**를 클릭합니다.

단계 **3** 표시되는 **New Network Device Profile(**새 네트워크 디바이스 프로파일**)** 창에서 네트워크 디바이스의 **Name(**이름**)** 및 **Description(**설명**)** 필드에 해당 값을 입력합니다.

단계 **4** 드롭다운 목록에서 네트워크 디바이스의 벤더를 선택합니다.

단계 **5** 아이콘 영역에서 아이콘 변경 **...** 버튼을 클릭하여 시스템의 네트워크 디바이스 아이콘을 업로드합니다.

Cisco ISE에서 제공하는 기본 아이콘을 사용하려면 아이콘 영역에서**Set To Default(**기본값으로 설정**)** 버튼을 클릭합니다.

단계 **6** **Supported Protocols(**지원되는 프로토콜**)** 영역에서 디바이스가 지원하는 프로토콜의 확인란을 선택합니다. 실제로 사용하려는 프로토콜에 대해서만 확인란을 선택합니다. 디바이스가 RADIUS 프로토콜을 지원하는 경우 **RADIUS Dictionaries(RADIUS** 사전**)** 드롭다운 목록에서 디바이스와 함께 사용할 RADIUS 사전을 선택합니다.

단계 **7** **Templates(**템플릿**)** 영역에서 다음과 같이 관련 세부정보를 입력합니다.

a) **Authentication/Authorization(**인증/권한 부여**)** 섹션을 펼쳐 플로우 유형, 속성 별칭 및 호스트 조회에 대한 디바이스의 기본 설정을 구성합니다. 표시되는 새 **Flow Type Conditions(**플로우 유형 조건**)** 영역에서 디바이스가 Wired MAB 또는 802.1X와 같은 다양한 인증 및 권한 부여 플로우에 사용하는 속성 및 값을 입력합니다. 그러면 Cisco ISE가 사용하는 속성에 따라 디바이스에 적합한 플로우 유형을 탐지할 수 있습니다. MAB에 대한 IETF 표준은 없으며, 벤더마다 Service-Type에 각기 다른 값을 사용합니다. 올바른 설정을 확인하려면 디바이스의 사용 설명서를 참고하거나 MAB 인증의 스니퍼 추적을 사용합니다. **Attribute Aliasing(**속성 별칭**)** 영역에서 정책 규칙을 간소화하기 위해 디바이스별 속성 이름을 공용 이름에 매핑합니다. 현재는 SSID(Service Set Identifier)만 정의되어 있습니다. 네트워크 디바이스에 무선 SSID 개념이 있는 경우 이를 디바이스가 사용하는 속성으로 설정합니다. Cisco ISE는 이를 정규화된 RADIUS 사전 내의 SSID라는 속성에 매핑합니다. 이렇게 하면 규칙 하나에서 SSID를 참조할 수 있으며, 기본 속성이 다르더라도 해당 규칙이 여러 디바이스에서 작동하므로 정책 규칙 컨피그레이션을 간소화할 수 있습니다. **Host Lookup(**호스트 조회**)** 영역에서 **Process Host Lookup(**프로세스 호스트 조회**)** 확인란을 선택하고 서드파티 지침에 따라 디바이스에 대해 관련 MAB 프로토콜 및 속성을 선택합니다.

b) **Permissions(**권한**)** 접힘 메뉴를 클릭해서 VLAN 및 ACL에 대한 네트워크 디바이스의 기본 설정을 구성합니다. 이러한 설정은 Cisco ISE에서 생성한 권한 부여 프로파일을 기준으로 하여 자동으로 매핑됩니다.

c) 네트워크 디바이스의 CoA 기능을 구성하려면 **CoA(Change of Authorization)** 접힘 메뉴를 클릭합니다.

d) 디바이스의 URL 리디렉션 기능을 구성하려면 **Redirect(**리디렉션**)** 섹션을 펼칩니다. URL 리디렉션은 게스트, BYOD 및 포스처 서비스에 필요합니다.

단계 **8** **Submit(**제출**)**을 클릭합니다.

관련 항목

ISE 네트워크 액세스 디바이스 프로파일을 생성하는 방법

Cisco ISE에서 네트워크 디바이스 프로파일 내보내기

Cisco ISE에 구성된 단일 또는 여러 네트워크 디바이스 프로파일을 XML 파일 형식으로 내 보냅니다. 그런 다음 XML 파일을 편집하여 새 네트워크 프로파일로 Cisco ISE 파일에 가져올 수 있습니다.

시작하기 전에

ISE 네트워크 액세스 디바이스 프로파일을 생성하는 방법을 참조하십시오.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Network Resources(**네트워크 리소스**)** > **Network Device Profiles(**네트워크 디바이스 프로파일**)**를 선택합니다.

단계 **2** 내보낼 디바이스 옆의 확인란을 선택하고 **Export Selected(**선택 항목 내보내기**)**를 선택합니다.

단계 **3** **DeviceProfiles.xml** 파일이 로컬 하드 디스크에 다운로드됩니다.

Cisco ISE로 네트워크 디바이스 프로파일 가져오기

Cisco ISE XML 구조인 XML 파일 하나를 사용하여 네트워크 디바이스 프로파일 하나 또는 여러 개를 Cisco ISE로 가져옵니다. 가져온 여러 개의 파일에서 네트워크 디바이스 프로파일을 동시에 가져올 수는 없습니다.

일반적으로는 먼저 템플릿으로 사용할 기존 프로파일을 Cisco ISE 관리자 포털에서 내보냅니다. 파일에 디바이스 프로파일 세부정보를 필요한 대로 입력하고 XML 파일로 저장합니다. 그런 다음 수정한 파일을 다시 Cisco ISE로 가져옵니다. 여러 네트워크 디바이스 프로파일로 작업하려면 하나의 XML 파일로 구성된 다수의 프로파일을 내보내고 파일을 편집한 다음, 해당 프로파일을 함께 가져와 Cisco ISE에서 여러 프로파일을 생성하면 됩니다.

네트워크 디바이스 프로파일을 가져오는 동안에는 새 기록 생성만 할 수 있습니다. 기존 프로파일을 덮어쓸 수는 없습니다. 기존 네트워크 디바이스 프로파일을 업데이트하려면 Cisco ISE에서 기존 프로파일을 내보내고 Cisco ISE에서 프로파일을 삭제한 다음, 적절하게 편집한 후 프로파일을 가져옵니다.

시작하기 전에

ISE 네트워크 액세스 디바이스 프로파일을 생성하는 방법을 참조하십시오.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Network Resources(**네트워크 리소스**)** > **Network Device Profiles(**네트워크 디바이스 프로파일**)**를 선택합니다.

단계 **2** **Import(**가져오기**)**를 클릭합니다.

단계 **3** **Choose File(**파일 선택**)**을 클릭하여 클라이언트 브라우저를 실행 중인 시스템에서 XML 파일을 선택합니다.

단계 **4** **Import(**가져오기**)**를 클릭합니다.

네트워크 디바이스 그룹 관리

다음 창에서는 네트워크 디바이스 그룹을 구성하고 관리할 수 있습니다.

네트워크 디바이스 그룹 설정

다음 표에서는 네트워크 디바이스 그룹을 생성하는 데 사용할 수 있는 **Network Device Groups(**네트워크 디바이스 그룹**)** 창의 필드에 대해 설명합니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Network Resources(**네트워크 리소스**)** > **Network Device Groups(**네트워크 디바이스 그룹**)** > **All Groups(**모든 그룹**)**입니다.

Work Centers(작업 센터**)** > **Device Administration(**디바이스 관리**)** > **Network Resources(**네트워크 리소스**)** > **Network Device Groups(**네트워크 디바이스 그룹**)** > **All Groups(**모든 그룹**)** 창에서 네트워크 디바이스 그룹을 생성할 수도 있습니다.

표 ***9: Network Device Group(***네트워크 디바이스 그룹***)*** 창의 필드

필드 이름	사용 지침
Name(이름**)**	루트 네트워크 디바이스 그룹의 이름을 입력합니다. 루트 네트워크 디바이스 그룹에 추가된 모든 후속 자식 네트워크 디바이스 그룹에 대해서는 새롭게 생성된 네트워크 디바이스 그룹의 이름을 입력합니다. 루트 노드를 포함하여 네트워크 디바이스 그룹 계층 구조에 최대 6개의 노드를 포함할 수 있습니다. 각 네트워크 디바이스 그룹의 이름은 최대 32자까지 지정할 수 있습니다.
Description(설명**)**	루트 또는 자식 네트워크 디바이스 그룹에 대한 설명을 입력합니다.
No. of Network Devices(네트워크 디바이스 수**)**	이 열에 네트워크 그룹의 네트워크 디바이스 수가 표시됩니다.

네트워크 디바이스 그룹 가져오기 설정

다음 표에서는 **Network Device Group(**네트워크 디바이스 그룹**)** 창의 **Import(**가져오기**)** 대화 상자에 대해 설명합니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Network Resources(**네트워크 리소스**)** > **Network Device Groups(**네트워크 디바이스 그룹**)**입니다.

표 ***10: Network Device Groups Import(***네트워크 디바이스 그룹 가져오기***)*** 창의 필드

필드 이름	사용 지침
Generate a Template(템플릿 생성**)**	링크를 클릭하여 CSV 템플릿 파일을 다운로드합니다. 네트워크 디바이스 그룹 정보가 포함된 템플릿을 같은 형식으로 업데이트하여 로컬에 저장하면 해당 네트워크 디바이스 그룹을 Cisco ISE 구축으로 가져올 수 있습니다.
File(파일**)**	업로드할 CSV 파일의 위치로 **Choose File(**파일 선택**)**을 클릭합니다. 이 파일은 새로 생성된 파일이거나 다른 Cisco ISE 구축에서 이전에 내보낸 파일일 수 있습니다. Cisco ISE 구축에서 신규/업데이트된 네트워크 디바이스 그룹 정보가 포함된 다른 구축으로 네트워크 디바이스 그룹을 가져올 수 있습니다.

필드 이름	사용 지침
Overwrite Existing Data with New Data(새 데이터로 기존 데이터 덮어쓰기**)**	Cisco ISE가 기존 네트워크 디바이스 그룹을 가져온 파일의 디바이스 그룹으로 교체하도록 하려면 **Overwrite Existing Data with New Data(**새 데이터로 기존 데이터 덮어쓰기**)** 확인란을 선택합니다. 이 확인란을 선택하지 않으면 가져온 파일에서 새 네트워크 디바이스 그룹이 네트워크 디바이스 그룹 저장소에 추가됩니다. 중복 엔트리는 무시됩니다.
Stop Import on First Error(첫 번째 오류에서 가져오기 중지**)**	가져오기 중에 오류가 발생한 첫 번째 인스턴스에서 가져오기를 중단하려면 **Stop Import on First Error(**첫 번째 오류에서 가져오기 중지**)** 확인란을 선택합니다. 이 확인란을 선택하지 않은 상태에서 오류가 발생하면 Cisco ISE가 오류를 보고하고 디바이스 그룹에 속한 나머지를 계속 가져옵니다.

네트워크 디바이스 그룹

Cisco ISE에서는 네트워크 디바이스를 포함하는 계층적 NDG(Network Device Groups)를 생성할 수 있습니다. NDG에서는 지리적 위치, 디바이스 유형 및 네트워크의 상대적 위치(예: "액세스 레이어" 또는 "데이터 센터")와 같은 다양한 기준에 따라 네트워크 디바이스를 논리적으로 그룹화합니다.

NDG 창을 보려면 **Menu(**메뉴**)** 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Network Resources(**네트워크 리소스**)** > **Network Device Groups(**네트워크 디바이스 그룹**)**를 .

예를 들어 지리적 위치별로 네트워크 디바이스를 구성하려는 경우 다음과 같이 대륙, 지역 및 국가별로 디바이스를 그룹화할 수 있습니다.

- 아프리카 > 남부 > 나미비아
- 아프리카 > 남부 > 남아프리카
- 아프리카 > 남부 > 보츠와나

디바이스 유형에 따라 네트워크 디바이스를 그룹화할 수 있습니다.

- 아프리카 > 남부 > 보츠와나 > 방화벽
- 아프리카 > 남부 > 보츠와나 > 라우터
- 아프리카 > 남부 > 보츠와나 > 스위치

하나 이상의 계층적 네트워크 디바이스 그룹에 네트워크 디바이스를 할당합니다. 따라서 Cisco ISE가 특정 디바이스에 할당할 적절한 그룹을 확인하기 위해 구성된 NDG의 순서가 지정된 목록을 살펴볼 때 같은 디바이스 프로파일이 여러 디바이스 그룹에 적용되어 있음을 확인할 수 있습니다. 이 경우 Cisco ISE는 일치하는 첫 번째 디바이스 그룹을 적용합니다.

생성할 수 있는 네트워크 디바이스 그룹의 최대 수에는 제한이 없습니다. 네트워크 디바이스 그룹에 대해 최대 6개 레벨의 계층 구조(상위 그룹 포함)를 생성 할 수 있습니다.

디바이스 그룹 계층 구조는 **Tree Table(**트리 표**)** 및 **Flat Table(**플랫 표**)**의 두 가지 보기로 표시됩니다. 네트워크 디바이스 그룹 목록 위의 **Tree Table(**트리 표**)** 또는 **Flat Table(**플랫 표**)**을 클릭하여 원하는 보기로 목록을 구성합니다.

Tree Table(트리 표**)** 보기에서는 루트 노드가 트리의 맨 위에 나타나며 그 뒤에 하위 그룹이 계층 구조로 나타납니다. 각 루트 그룹의 모든 디바이스 그룹을 보려면 **Expand All(**모두 확장**)**을 클릭합니다. 루트 그룹만 목록으로 보려면 **Collapse All(**모두 축소**)**를 클릭합니다.

Flat Table(플랫 표**)** 보기에서는 각 디바이스 그룹의 계층 구조가 **Group Hierarchy(**그룹 계층 구조**)** 열에 표시됩니다.

두 보기 모두에서 각 하위 그룹에 할당된 네트워크 디바이스의 수가 해당하는 **No. of Network Devices(**네트워크 디바이스 수**)** 열에 표시됩니다. 이 숫자를 클릭하면 해당 디바이스 그룹에 할당된 모든 네트워크 디바이스가 나열된 대화 상자가 실행됩니다. 표시되는 대화 상자에는 네트워크 디바이스를 한 그룹에서 다른 그룹으로 이동할 수 있는 두 개의 버튼도 있습니다. 네트워크 그룹을 현재 그룹에서 다른 그룹으로 이동하려면 **Move Devices to Another Group(**디바이스를 다른 그룹으로 이동**)** 버튼을 클릭합니다. **Add Devices to Group(**그룹에 디바이스 추가**)** 버튼을 클릭하여 네트워크 디바이스를 선택한 네트워크 디바이스 그룹으로 이동합니다.

Network Device Groups(네트워크 디바이스 그룹**)** 창에서 네트워크 디바이스 그룹을 추가하려면 **Add(**추가**)**를 클릭합니다. **Parent Group(**상위 그룹**)** 드롭 다운 목록에서 네트워크 디바이스 그룹을 추가해야 하는 상위 그룹을 선택하거나 **Add As Root Group(**루트 그룹으로 추가**)** 옵션을 선택하여 새 네트워크 디바이스 그룹을 상위 그룹으로 추가합니다.

참고 해당 디바이스 그룹에 디바이스가 할당되어 있으면 디바이스 그룹을 삭제할 수 없습니다. 디바이스 그룹을 삭제하기 전에 모든 기존 디바이스를 다른 디바이스 그룹으로 이동해야 합니다.

루트 네트워크 디바이스 그룹

Cisco ISE에는 **All Device Types(**모든 디바이스 유형**)** 및 **All Locations(**모든 위치**)**의 두 가지 미리 정의된 루트 네트워크 디바이스 그룹이 포함되어 있습니다. 이러한 미리 정의된 네트워크 디바이스 그룹을 편집, 복제 또는 삭제할 수는 없지만 그 아래에 새 디바이스 그룹을 추가할 수는 있습니다.

이전 섹션에서 설명한 대로 루트 네트워크 디바이스 그룹(네트워크 디바이스 그룹)을 생성 한 다음 **Network Device Groups(**네트워크 디바이스 그룹**)** 창의 루트 그룹 아래에 하위 네트워크 디바이스 그룹을 생성할 수 있습니다.

정책 평가에서 Cisco ISE가 사용하는 네트워크 디바이스 속성

새 네트워크 디바이스 그룹을 생성할 때는 새 네트워크 디바이스 속성이 **System Dictionaries(**시스템 사전**)**의 **Device(**디바이스**)** 사전에 추가됩니다**(Policy(**정책**)** > **Policy Elements(**정책 요소**)** > **Dictionaries(**사전**))**. 그러면 추가된 디바이스 속성이 정책 정의에 사용됩니다.

Cisco ISE에서는 디바이스 유형, 위치, 모델 이름 및 네트워크 디바이스에서 실행 중인 소프트웨어 버전과 같은 디바이스 사전 속성을 기준으로 인증 및 권한 부여 정책을 구성할 수 있습니다.

Cisco ISE로 네트워크 디바이스 그룹 가져오기

CSV(comma-separated value) 파일을 사용하여 Cisco ISE 노드로 네트워크 디바이스 그룹을 가져올 수 있습니다. 서로 다른 두 가져오기 파일에서 네트워크 디바이스 그룹을 동시에 가져올 수는 없습니다.

Cisco ISE 관리자 포털에서 CSV 템플릿을 다운로드하고 해당 템플릿에 네트워크 디바이스 그룹 세부정보를 입력한 후에 템플릿을 CSV 파일로 저장합니다. 그런 다음 편집한 파일을 Cisco ISE로 가져오면 됩니다.

디바이스 그룹을 가져올 때 새 기록을 생성하거나 기존 기록을 업데이트할 수 있습니다. 디바이스 그룹을 가져올 때는 Cisco ISE가 기존 디바이스 그룹을 새 그룹으로 덮어쓰도록 할지 아니면 Cisco ISE에서 첫 번째 오류를 발견할 때 가져오기 프로세스를 중지하도록 할지를 정의할 수도 있습니다.

단계 **1** Cisco ISE GUI에서 메뉴아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Network Resources(**네트워크 리소스**)** > **Network Device Groups(**네트워크 디바이스 그룹**)**를 선택합니다.

단계 **2** **Import(**가져오기**)**를 클릭합니다.

단계 **3** 대화 상자가 표시되면 **Choose File(**파일 선택**)**을 클릭하여 클라이언트 브라우저를 실행 중인 시스템에서 CSV 파일을 선택합니다.

네트워크 디바이스 그룹을 추가하는 데 필요한 CSV 템플릿 파일을 다운로드하려면 **Generate a Template(**템플릿 생성**)**을 클릭합니다.

단계 **4** 기존 네트워크 디바이스 그룹을 덮어쓰려면 **Overwrite Existing Data with New Data(**새 데이터로 기존 데이터 덮어쓰기**)** 확인란을 선택합니다.

단계 **5** **Stop Import on First Error(**첫 번째 오류에서 가져오기 중지**)** 확인란을 선택합니다.

단계 **6** **Import(**가져오기**)**를 클릭합니다.

Cisco ISE에서 네트워크 디바이스 그룹 내보내기

Cisco ISE에 구성된 네트워크 디바이스 그룹을 CSV 파일 형식으로 내보낼 수 있습니다. 그런 다음 이러한 네트워크 디바이스 그룹을 다른 Cisco ISE 노드로 가져올 수 있습니다.

단계 **1** Cisco ISE GUI에서 **Menu(**메뉴**)** 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Network Resources(**네트워크 리소스**)** > **Network Device Groups(**네트워크 디바이스 그룹**)** > **All Groups(**모든 그룹**)**를 선택합니다.

단계 **2** 네트워크 디바이스 그룹을 내보내려는 경우 다음 중 하나를 수행할 수 있습니다.

- 내보낼 디바이스 그룹 옆의 확인란을 선택하고 **Export(**내보내기**)** > **Export Selected(**선택 항목 내보내기**)**를 선택합니다.
- 정의되어 있는 모든 네트워크 디바이스 그룹을 내보내려면 **Export(**내보내기**)** > **Export All(**모두 내보내기**)**을 선택합니다.

단계 **3** CSV 파일이 로컬 하드 디스크에 다운로드됩니다.

네트워크 디바이스 그룹 관리

다음 창에서는 네트워크 디바이스 그룹을 구성하고 관리할 수 있습니다.

네트워크 디바이스 그룹 설정

다음 표에서는 네트워크 디바이스 그룹을 생성하는 데 사용할 수 있는 **Network Device Groups(**네트워크 디바이스 그룹**)** 창의 필드에 대해 설명합니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Network Resources(**네트워크 리소스**)** > **Network Device Groups(**네트워크 디바이스 그룹**)** > **All Groups(**모든 그룹**)**입니다.

Work Centers(작업 센터**)** > **Device Administration(**디바이스 관리**)** > **Network Resources(**네트워크 리소스**)** > **Network Device Groups(**네트워크 디바이스 그룹**)** > **All Groups(**모든 그룹**)** 창에서 네트워크 디바이스 그룹을 생성할 수도 있습니다.

표 ***11: Network Device Group(***네트워크 디바이스 그룹***)*** 창의 필드

필드 이름	사용 지침
Name(이름**)**	루트 네트워크 디바이스 그룹의 이름을 입력합니다. 루트 네트워크 디바이스 그룹에 추가된 모든 후속 자식 네트워크 디바이스 그룹에 대해서는 새롭게 생성된 네트워크 디바이스 그룹의 이름을 입력합니다. 루트 노드를 포함하여 네트워크 디바이스 그룹 계층 구조에 최대 6개의 노드를 포함할 수 있습니다. 각 네트워크 디바이스 그룹의 이름은 최대 32자까지 지정할 수 있습니다.
Description(설명**)**	루트 또는 자식 네트워크 디바이스 그룹에 대한 설명을 입력합니다.
No. of Network Devices(네트워크 디바이스 수**)**	이 열에 네트워크 그룹의 네트워크 디바이스 수가 표시됩니다.

네트워크 디바이스 그룹 가져오기 설정

다음 표에서는 **Network Device Group**(네트워크 디바이스 그룹) 창의 **Import**(가져오기) 대화 상자에 대해 설명합니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Administration**(관리) > **Network Resources**(네트워크 리소스) > **Network Device Groups**(네트워크 디바이스 그룹)입니다.

표 ***12: Network Device Groups Import***(네트워크 디바이스 그룹 가져오기) 창의 필드

필드 이름	사용 지침
Generate a Template(템플릿 생성)	링크를 클릭하여 CSV 템플릿 파일을 다운로드합니다. 네트워크 디바이스 그룹 정보가 포함된 템플릿을 같은 형식으로 업데이트하여 로컬에 저장하면 해당 네트워크 디바이스 그룹을 Cisco ISE 구축으로 가져올 수 있습니다.
File(파일)	업로드할 CSV 파일의 위치로 **Choose File**(파일 선택)을 클릭합니다. 이 파일은 새로 생성된 파일이거나 다른 Cisco ISE 구축에서 이전에 내보낸 파일일 수 있습니다. Cisco ISE 구축에서 신규/업데이트된 네트워크 디바이스 그룹 정보가 포함된 다른 구축으로 네트워크 디바이스 그룹을 가져올 수 있습니다.
Overwrite Existing Data with New Data(새 데이터로 기존 데이터 덮어쓰기)	Cisco ISE가 기존 네트워크 디바이스 그룹을 가져온 파일의 디바이스 그룹으로 교체하도록 하려면 **Overwrite Existing Data with New Data**(새 데이터로 기존 데이터 덮어쓰기) 확인란을 선택합니다. 이 확인란을 선택하지 않으면 가져온 파일에서 새 네트워크 디바이스 그룹이 네트워크 디바이스 그룹 저장소에 추가됩니다. 중복 엔트리는 무시됩니다.
Stop Import on First Error(첫 번째 오류에서 가져오기 중지)	가져오기 중에 오류가 발생한 첫 번째 인스턴스에서 가져오기를 중단하려면 **Stop Import on First Error**(첫 번째 오류에서 가져오기 중지) 확인란을 선택합니다. 이 확인란을 선택하지 않은 상태에서 오류가 발생하면 Cisco ISE가 오류를 보고하고 디바이스 그룹에 속한 나머지를 계속 가져옵니다.

Cisco ISE에서 템플릿 가져오기

Cisco ISE에서는 CSV 파일을 사용하여 많은 네트워크 디바이스 및 네트워크 디바이스 그룹을 가져올 수 있습니다. 템플릿은 필드의 형식을 정의하는 헤더 행을 포함합니다. 이 헤더 행을 편집해서는 안 됩니다.

네트워크 디바이스 및 네트워크 디바이스 그룹에 대한 해당 가져오기 플로우에서 **Generate a Template(**템플릿 생성**)** 링크를 사용하여 CSV 파일을 로컬 시스템에 저장할 수 있습니다.

네트워크 디바이스 가져오기 템플릿 형식

다음 표는 가져오기 네트워크 디바이스 CSV 템플릿 파일의 헤더에 있는 필드를 나열하고 그에 대한 설명을 제공합니다.

표 ***13: CSV*** 템플릿 필드 및 네트워크 디바이스에 대한 설명

필드	설명
Name:String(32)(이름**:**문자열**(32))**	(필수) 네트워크 디바이스 이름 필드입니다. 최대 길이가 32자인 영숫자 문자열입니다.
Description:String(256)(설명**:**문자열**(256))**	네트워크 디바이스에 대한 설명입니다. 최대 길이가 256자인 문자열입니다.
IP Address:Subnets(a.b.c.d/m|...)(IP 주소**:**서브넷**(a.b.c.d/m|...))**	(필수) 네트워크 디바이스의 IP 주소 및 서브넷 마스크 필드입니다. 둘 이상의 값을 파이프("|") 기호로 구분하여 포함할 수 있습니다. IPv4 및 IPv6 네트워크 디바이스(TACACS 및 RADIUS) 컨피그레이션 및 외부 RADIUS 서버 컨피그레이션에 지원됩니다. IPv4 주소를 입력할 때 범위 및 서브넷 마스크를 사용할 수 있습니다.
Model Name:String(32)(모델 이름**:**문자열**(32))**	(필수) 네트워크 디바이스 모델 이름 필드입니다. 최대 길이가 32자인 문자열입니다.
Software Version:String(32)(소프트웨어 버전**:**문자열**(32))**	(필수) 네트워크 디바이스 소프트웨어 버전 필드입니다. 최대 길이가 32자인 문자열입니다.
Network Device Groups:String(100)(네트워크 디바이스 그룹**:**문자열**(100))**	(필수) 이 필드에는 기존 네트워크 디바이스 그룹을 입력해야 합니다. 하위 그룹이지만 상위 그룹과 하위 그룹을 쉼표로 구분하여 모두 포함해야 합니다. 최대 길이가 100자인 문자열입니다. 예를 들어 *Location>All Location>US*입니다.

필드	설명
Authentication:Protocol:String(6)(인증**:**프로토콜**:** 문자열**(6))**	이 필드는 사용하고자 하는 인증 프로토콜을 나타냅니다. 유효한 값은 "RADIUS"(대/소문자 구분 안 함)뿐입니다.
Authentication:Shared Secret:String(128)(인증**:** 공유 암호**:**문자열**(128))**	(인증 프로토콜 필드에 값을 입력하는 경우 필수) 이 필드의 값은 최대 길이가 128자인 문자열입니다.
EnableKeyWrap:Boolean(true|false)(EnableKeyWrap: 부울**(true|false))**	이 필드는 네트워크 디바이스에서 지원되는 경우에만 활성화됩니다. 유효한 값은 "true" 및 "false"입니다.
EncryptionKey:String(ascii:16|hexa:32)(EncryptionKey: 문자열**(ascii:16|16**진수**:32))**	(KeyWrap을 활성화하는 경우 필수) 이 필드는 세션 암호화에 사용되는 암호화 키를 나타냅니다. ASCII 값: 길이가 16자(바이트)입니다. 16진수 값: 길이가 32자(바이트)입니다.
AuthenticationKey:String(ascii:20|hexa:40)(AuthenticationKey: 문자열**(ascii:20|16**진수**:40))**	(KeyWrap을 활성화하는 경우 필수) 이 필드는 RADIUS 메시지에 대한 키 HMAC(Hashed Message Authentication Code) 계산을 나타냅니다. ASCII 값: 길이가 20자(바이트)입니다. 16진수 값: 길이가 40자(바이트)입니다.
InputFormat:String(32)(InputFormat:문자열**(32))**	이 필드는 암호화 및 인증 키 입력 형식을 나타냅니다. ASCII 및 16진수 값이 허용됩니다.
SNMP:Version:Enumeration (|2c|3)(SNMP:버전**:** 열거**(|2c|3))**	이 필드는 프로파일러 서비스에서 사용하는 필드입니다. SNMP 프로토콜의 버전 1, 2c 또는 3입니다.
SNMP:RO Community:String(32)(SNMP:RO 커뮤니티**:**문자열**(32))**	(SNMP Version(SNMP 버전) 필드에 값을 입력하는 경우 필수) SNMP 읽기 전용 커뮤니티입니다. 이 필드는 최대 길이가 32자인 문자열을 나타냅니다.
SNMP:RW Community:String(32)(SNMP:RW 커뮤니티**:**문자열**(32))**	(SNMP Version(SNMP 버전) 필드에 값을 입력하는 경우 필수) SNMP 읽기/쓰기 커뮤니티입니다. 이 필드는 최대 길이가 32자인 문자열을 나타냅니다.
SNMP:Username:String(32)(SNMP:사용자 이름**:** 문자열**(32))**	이 필드는 최대 길이가 32자인 문자열을 나타냅니다.

필드	설명
SNMP:Security Level:Enumeration(Auth|No Auth|Priv)(SNMP:보안 레벨**:**열거**(**인증**|**인증 안 함**|**개인**))**	(SNMP 버전 3을 선택하는 경우 필수) 이 필드는 "Auth(인증)", "No Auth(인증 안 함)", "Priv(개인)" 값을 허용합니다.
SNMP:Authentication Protocol:Enumeration(MD5|SHA)(SNMP:인증 프로토콜**:**열거**(MD5|SHA))**	(SNMP 보안 레벨로 인증 또는 개인을 입력한 경우 필수) 이 필드는 "MD5" 또는 "SHA" 값을 허용합니다.
SNMP:Authentication Password:String(32)(SNMP:인증 비밀번호**:**문자열**(32))**	(SNMP 보안 레벨로 Auth(인증)를 입력한 경우 필수) 이 필드는 최대 길이가 32자인 문자열을 나타냅니다.
SNMP:Privacy Protocol:Enumeration(DES|AES128|AES192|AES256|3DES)(SNMP:프라이버시 프로토콜**:**열거**(DES|AES128|AES192|AES256|3DES))**	(SNMP 보안 레벨로 개인을 입력한 경우 필수) 이 필드는 "DES", "AES128", "AES192", "AES256" 또는 "3DES" 값을 허용합니다.
SNMP:Privacy Password:String(32)(SNMP:프라이버시 비밀번호**:**문자열**(32))**	(SNMP 보안 레벨로 "Priv"(개인)를 입력한 경우 필수) 이 필드는 최대 길이가 32자인 문자열을 나타냅니다.
SNMP:Polling Interval:Integer:600-86400 seconds(SNMP:폴링 간격**:**정수**:600-86,400**초**)**	이 필드는 SNMP 폴링 간격 설정을 위한 필드입니다. 유효한 값은 600~86400의 정수입니다.
SNMP:Is Link Trap Query:Boolean(true|false)(SNMP:링크 트랩 쿼리 여부**:**부울**(true|false))**	SNMP 링크 트랩을 활성화 또는 비활성화하기 위한 필드입니다. 유효한 값은 "true" 또는 "false"입니다.
SNMP:Is MAC Trap Query:Boolean(true|false)(SNMP:MAC 트랩 쿼리 여부**:**부울**(true|false))**	이 필드는 SNMP MAC 트랩을 활성화 또는 비활성화하기 위한 필드입니다. 유효한 값은 "true" 또는 "false"입니다.
SNMP:Originating Policy Services Node:String(32)(SNMP:원래 정책 서비스 노드**:**문자열**(32))**	이 필드는 SNMP 데이터를 폴링하는 데 사용해야 하는 ISE 서버를 나타냅니다. 기본적으로는 자동 설정되지만 다른 값을 이 필드에 할당하여 설정을 덮어쓸 수 있습니다.
Trustsec:Device Id:String(32)(Trustsec:디바이스 **ID:**문자열**(32))**	이 필드는 Cisco Trustsec 디바이스 ID를 나타내며 최대 길이가 32자인 문자열입니다.
Trustsec:Device Password:String(256)(Trustsec: 디바이스 비밀번호**:**문자열**(256))**	(Cisco TrustSec 디바이스 ID를 입력한 경우 필수) 이 필드는 Cisco TrustSec 디바이스 비밀번호를 나타내며 최대 길이가 256자인 문자열입니다.

필드	설명
Trustsec:Environment Data Download Interval:Integer:1-2147040000 seconds(Trustsec: 환경 데이터 다운로드 간격**:**정수**:1-2,147,040,000** 초**)**	이 필드는 Cisco TrustSec 환경 데이터 다운로드 간격을 설정하는 필드입니다. 유효한 값은 1~24850의 정수입니다.
Trustsec:Peer Authorization Policy Download Interval:Integer:1-2147040000 seconds(Trustsec: 피어 권한 부여 정책 다운로드 간격**:**정수**:1-2,147,040,000**초**)**	이 필드는 Cisco TrustSec 피어 권한 부여 정책 다운로드 간격을 설정하는 필드입니다. 유효한 값은 1~24850의 정수입니다.
Trustsec:Reauthentication Interval:Integer:1-2147040000 seconds(Trustsec: 재인증 간격**:**정수**:1-2,147,040,000**초**)**	이 필드는 Cisco TrustSec 재인증 간격을 설정하는 필드입니다. 유효한 값은 1~24850의 정수입니다.
Trustsec:SGACL List Download Interval:Integer:1-2147040000 seconds(Trustsec:SGACL 목록 다운로드 간격**:**정수**:1-2,147,040,000**초**)**	이 필드는 Cisco TrustSec 보안 그룹 ACL 목록 다운로드 간격을 설정하는 필드입니다. 유효한 값은 1~24850의 정수입니다.
Trustsec:Is Other Trustsec Devices Trusted:Boolean(true|false)(Trustsec:다른 **Trustsec** 디바이스 신뢰 여부**:**부울**(true|false))**	이 필드는 Cisco TrustSec 디바이스의 신뢰 여부를 나타냅니다. 유효한 값은 "true" 또는 "false"입니다.
Trustsec:Notify this device about Trustsec configuration changes:String(ENABLE_ALL|DISABLE_ALL)(Trustsec:Trustsec 컨피그레이션 변경사항을 이 디바이스에 알림**:**문자열**(ENABLE_ALL|DISABLE_ALL))**	이 필드는 Cisco TrustSec 디바이스의 Cisco TrustSec 컨피그레이션 변경사항을 알립니다. 유효한 값은 **ENABLE_ALL** 또는 **DISABLE_ALL**입니다.
Trustsec:Include this device when deploying Security Group Tag Mapping Updates:Boolean(true|false)(Trustsec:보안 그룹 태그 매핑 업데이트 구축 시 이 디바이스 포함**:**부울**(true|false))**	이 필드는 Cisco TrustSec 디바이스가 보안 그룹 태그에 포함되어 있는지 여부를 나타냅니다. 유효한 값은 "true" 또는 "false"입니다.
Deployment:Execution Mode Username:String(32)(구축**:**실행 모드 사용자 이름**:**문자열**(32))**	이 필드는 디바이스 컨피그레이션 편집 권한이 있는 사용자 이름을 나타냅니다. 최대 길이가 32자인 문자열입니다.
Deployment:Execution Mode Password:String(32)(구축**:**실행 모드 비밀번호**:**문자열**(32))**	이 필드는 디바이스 비밀번호를 나타내며 최대 길이가 32자인 문자열입니다.
Deployment:Enable Mode Password:String(32)(구축**:**활성화 모드 비밀번호**:**문자열**(32))**	이 필드는 컨피그레이션을 수정할 수 있는 디바이스의 비밀번호를 나타냅니다. 최대 길이가 32자인 문자열입니다.

필드	설명
Trustsec:PAC issue date:Date(Trustsec:PAC 발급 날짜**:**날짜**)**	이 필드는 Cisco TrustSec 디바이스에 대해 Cisco ISE에서 마지막으로 생성한 Cisco TrustSec PAC의 발급 날짜를 표시합니다.
Trustsec:PAC expiration date:Date(Trustsec:PAC 만료 날짜**:**날짜**)**	이 필드는 Cisco TrustSec 디바이스에 대해 Cisco ISE에서 마지막으로 생성한 Cisco TrustSec PAC의 만료 날짜를 표시합니다.
Trustsec:PAC issued by:String(Trustsec:PAC 발급자**:**문자열**)**	이 필드는 Cisco TrustSec 디바이스에 대해 Cisco ISE에서 마지막으로 생성한 Cisco TrustSec PAC의 발급자 이름(Cisco TrustSec 관리자)을 표시합니다. 문자열 값입니다.

네트워크 디바이스 그룹 가져오기 템플릿 형식

다음 표에서는 템플릿 헤더의 필드를 소개하고 네트워크 디바이스 그룹 CSV 파일의 필드에 대해 설명합니다.

표 ***14: CSV*** 템플릿 필드 및 네트워크 디바이스 그룹에 대한 설명

필드	설명
Name:String(100)(이름:문자열(100)):	(필수) 네트워크 디바이스 그룹 이름 필드입니다. 최대 길이가 100자인 문자열입니다. NDG의 전체 이름은 최대 100자까지 지정할 수 있습니다. 예를 들어 Global(전 세계) > Asia(아시아) 부모 그룹 아래에 하위 그룹 India(인도)를 생성하는 경우 생성하는 NDG의 전체 이름은 Global#Asia#India이며 이 전체 이름의 길이는 100자를 초과할 수 없습니다. NDG의 전체 이름 길이가 100자를 초과하면 NDG 생성이 실패합니다.
Description:String(1024)(설명:문자열(1024))	네트워크 디바이스 그룹 설명(선택 사항)입니다. 최대 길이가 1,024자인 문자열입니다.
Type:String(64)(유형:문자열(64)):	(필수) 네트워크 디바이스 그룹 유형 필드입니다. 최대 길이가 64자인 문자열입니다.
Is Root:Boolean(true|false)(루트 여부:부울(true|false)):	(필수) 특정 네트워크 디바이스 그룹이 루트 그룹인지를 결정하는 필드입니다. 유효한 값은 true 또는 false입니다.

Cisco ISE와 NAD 간의 통신을 보호하기 위한 IPsec 보안

IPsec은 IP에 보안을 제공하는 프로토콜 집합입니다. AAA, RADIUS 및 TACACS+ 프로토콜은 MD5 해싱 알고리즘을 사용합니다. 보안 강화를 위해 Cisco ISE는 IPsec 기능을 제공합니다. IPsec은 발신자를 인증하고, 전송 중에 데이터의 변경 사항을 검색하고, 전송되는 데이터를 암호화하여 보안 통신을 제공합니다.

Cisco ISE는 터널 모드와 전송 모드에서 IPsec을 지원합니다. Cisco ISE 인터페이스에서 IPsec을 활성화하고 피어를 구성하면 Cisco ISE와 NAD 간에 IPsec 터널이 생성되어 통신을 보호합니다.

사전 공유 키를 정의하거나 IPsec 인증에 X.509 인증서를 사용할 수 있습니다. IPsec은 기가비트 이더넷 1 ~ 기가비트 이더넷 5 인터페이스에서 활성화할 수 있습니다. PSN 당 하나의 Cisco ISE 인터페이스에서만 IPsec을 구성할 수 있습니다.

스마트 라이선스가 기본적으로 활성화되어 있으므로(e0/2—> eth2) 기가비트 이더넷 2에서 IPsec을 활성화 할 수 없습니다. 그러나 IP 보안을 활성화해야 하는 경우 스마트 라이선싱을 위해 다른 인터페이스를 선택해야 합니다.

참고 기가비트 이더넷 0 및 본드 0(기가비트 이더넷 0 및 기가비트 이더넷 1 인터페이스가 결합 된 경우)은 Cisco ISE CLI의 관리 인터페이스입니다. IPsec은 기가비트 이더넷 0 및 본드 0에서 지원되지 않습니다.

필수 구성 요소

- Cisco ISE Release 2.2 및 그 이상
- Cisco IOS 소프트웨어, C5921 ESR 소프트웨어 (C5921_I86-UNIVERSALK9-M): ESR 5921 컨피그레이션은 기본적으로 터널 및 전송 모드에서 IPsec을 지원합니다. Diffie-Hellman Group 14와 Group 16이 지원됩니다.

참고 C5921 ESR 소프트웨어는 Cisco ISE 릴리스 2.2 이상과 함께 번들로 제공됩니다. 이를 활성화하려면 ESR 라이선스가 필요합니다. ESR 라이선싱 정보는 Cisco 5921 Embedded Services 라우터 통합 가이드를 참조하십시오.

Cisco ISE에서 RADIUS IPsec 구성

Cisco ISE에서 RADIUS IPsec을 구성하려면 다음을 수행해야합니다.

단계 **1** Cisco ISE CLI에서 인터페이스의 IP 주소를 구성합니다.

기가비트 이더넷 1 ~ 기가비트 이더넷 5 인터페이스(본드 1 및 본드 2)는 IPsec을 지원합니다. 그러나 Cisco ISE 노드의 인터페이스 하나에서만 IPsec을 구성 할 수 있습니다.

단계 **2** IPsec 네트워크 디바이스 그룹에 직접 연결된 네트워크 디바이스를 추가합니다.

참고 RADIUS IPsec을 사용하려면 디바이스의 인터페이스를 통해 고정 경로 게이트웨이를 직접 연결해야 합니다.

a) Cisco ISE GUI에서 **Menu(**메뉴**)** 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Network Resources(**네트워크 리소스**)** > **Network Devices(**네트워크 디바이스**)**를 .
b) **Networks Devices(**네트워크 디바이스**)** 창에서 **Add(**추가**)**를 클릭합니다.
c) 해당 필드에 추가할 네트워크 디바이스의 이름과 IP 주소 및 서브넷을 입력합니다.
d) IPSEC 드롭다운 목록에서 **Yes(**예**)**를 선택합니다.
e) **RADIUS Authentication Settings(RADIUS** 인증 설정**)** 확인란을 선택합니다.
f) **Shared Secret(**공유 암호**)** 필드에 네트워크 디바이스에서 구성한 공유 암호 키를 입력합니다.
g) **Save(**저장**)**를 클릭합니다.

단계 **3** Cisco SMSM(Smart Software Manager)과 상호 작용할 별도의 관리 인터페이스를 추가합니다. ESR(Embedded Services Router)에 대한 정보는 Smart Software Manager Satellite를 참조하십시오. 그렇게 하려면 Cisco ISE CLI에서 다음 명령을 실행하여 해당 관리 인터페이스(기가비트 이더넷 1 ~ 5 (또는 본드 1 또는 2))를 선택합니다.

ise/admin# **license esr smart** {*interface*}

이 인터페이스는 Cisco.com에 연결하여 Cisco 온라인 라이선싱 서버에 액세스할 수 있어야합니다

단계 **4** Cisco ISE CLI에서 직접 연결된 게이트웨이에 네트워크 디바이스를 추가합니다.

ip route [*destination network(*대상 네트워크*)*] [*network mask(*네트워크 마스트*)*] **gateway** [*next-hop address(*다음 홉 주소*)*]

단계 **5** Cisco ISE 노드에서 IPsec을 활성화합니다.

a) Cisco ISE GUI에서 **Menu(**메뉴**)** 아이콘(☰)을 **Administration(**관리**)** > **System(**시스템**)** > **Settings(**설정**)** > **Protocols(**프로토콜**)** > **IPSec**를 선택합니다.

구축의 모든 Cisco ISE 노드가이 창에 나열됩니다.

b) IPsec을 활성화하려는 Cisco ISE 노드 옆의 확인란을 선택하고 **Enable(**활성화**)** 라디오 버튼을 클릭합니다.
c) 선택한 노드의 **IPSec** 인터페이스: 드롭 다운 목록에서 IPsec 통신에 사용할 인터페이스를 선택합니다.
d) 선택한 Cisco ISE 노드에 대해 다음 인증 유형 중 하나의 라디오 버튼을 클릭합니다.

- **Pre-shared Key(**사전 공유 키**)**: 이 옵션을 선택하는 경우 사전 공유 키를 입력하고 네트워크 디바이스에서 동일한 키를 구성해야 합니다. 사전 공유 키에는 영숫자 문자를 사용합니다. 특수 문자는 사용할 수 없습니다 네트워크 디바이스에서 사전 공유 키를 구성하는 방법에 대한 지침은 네트워크 디바이스 설명서를 참조하십시오. 사전 공유 키 컨피그레이션 출력의 예는 예: Cisco Catalyst 3850 Series 스위치의 사전 공유 키 컨피그레이션 출력, 54 페이지의 내용을 참조하십시오.

- **X.509 Certificates(X.509** 인증서**)**: 이 옵션을 선택하는 경우 Cisco ISE CLI에서 ESR 셸로 이동하여 ESR 5921용 X.509 인증서를 구성 및 설치합니다. 그런 다음 IPsec용 네트워크 디바이스를 구성합니다. 자세한 내용은 ESR-5921에서 X.509 인증서 구성 및 설치, 49 페이지 섹션을 참조하십시오.

e) **Save(**저장**)**를 클릭합니다.

참고 IPsec 컨피그레이션을 직접 수정할 수 없습니다. IPsec이 활성화된 경우 IPsec 터널 또는 인증을 수정하려면 현재 IPsec 터널을 비활성화하고 IPsec 컨피그레이션을 수정한 다음 다른 컨피그레이션으로 IPsec 터널을 다시 활성화합니다.

참고 활성화되면 IPsec이 Cisco ISE 인터페이스에서 IP 주소를 제거하고 인터페이스를 종료합니다. 사용자가 Cisco ISE CLI에서 로그인하면 인터페이스가 IP 주소 없이 종료 상태로 표시됩니다. 이 IP 주소는 ESR-5921 인터페이스에서 구성됩니다.

단계 **6** **esr** 명령을 입력하여 ESR 쉘(shell)을 시작합니다.

```
ise/admin# esr
% Entering ESR 5921 shell
% Cisco IOS Software, C5921 Software (C5921_I86-UNIVERSALK9-M), Version 15.5(2)T2, RELEASE SOFTWARE (fc3)
% Technical Support: http://www.cisco.com/techsupport
% Copyright (c) 1986-2015 Cisco Systems, Inc.

Press RETURN to get started, CTRL-C to exit

ise-esr5921>
ise-esr5921>
```

참고 FIPS 규정 준수를 위해 8자 이상의 비밀번호를 구성해야 합니다. **Enable secret level 1** 명령을 입력하여 비밀번호를 지정합니다.

```
ise-esr5921(config)#enable secret level 1 ?
0 Specifies an UNENCRYPTED password will follow
5 Specifies a MD5 HASHED secret will follow
8 Specifies a PBKDF2 HASHED secret will follow
9 Specifies a SCRYPT HASHED secret will follow
LINE The UNENCRYPTED (cleartext) 'enable' secret
```

참고 GUI에서 사용자 맞춤화된 RADIUS 포트(1645, 1646, 1812, 1813 이외)를 구성하는 경우 구성된 RADIUS 포트를 수락하려면 ESR 셸에서 다음 CLI 명령을 입력해야합니다.

```
ip nat inside source static udp 10.1.1.2 [port_number] interface Ethernet0/0 [port_number]
```

단계 **7** IPsec 터널 및 IPsec 터널을 통한 RADIUS 인증을 확인합니다.

a) Cisco ISE에서 사용자를 추가하고 사용자를 사용자 그룹에 할당합니다(Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **Identities(ID)** > **Users(**사용자**)**를 선택합니다).

b) 다음 단계를 수행하여 Cisco ISE와 NAD 간에 IPsec 터널이 설정되었는지 확인합니다.

1. Cisco ISE와 NAD 간의 연결이 설정되었는지 테스트하려면 **ping** 명령을 사용합니다.
2. ESR 셸 또는 NAD CLI에서 다음 명령을 실행하여 연결이 활성 상태인지 확인합니다.

   show crypto isakmp sa

```
ise-esr5921#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
192.168.30.1    192.168.30.3    QM_IDLE           1001 ACTIVE
```

3. ESR 셸 또는 NAD CLI에서 다음 명령을 실행하여 터널이 설정되었는지 확인합니다.

   show crypto ipsec sa

```
ise-esr5921#show crypto ipsec sa

interface: Ethernet0/0
    Crypto map tag: radius, local addr 192.168.30.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.30.1/255.255.255.255/0/0)
   remote ident (addr/mask/prot/port): (192.168.30.2/255.255.255.255/0/0)
   current_peer 192.168.30.2 port 500
     PERMIT, flags={}
    #pkts encaps: 52, #pkts encrypt: 52, #pkts digest: 52
    #pkts decaps: 57, #pkts decrypt: 57, #pkts verify: 57
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 192.168.30.1, remote crypto endpt.: 192.168.30.2
     plaintext mtu 1438, path mtu 1500, ip mtu 1500, ip mtu idb Ethernet0/0
     current outbound spi: 0x393783B6(959939510)
     PFS (Y/N): N, DH group: none

     inbound esp sas:
      spi: 0x8EA0F6EE(2392913646)
        transform: esp-aes esp-sha256-hmac ,
        in use settings ={Tunnel, }
        conn id: 99, flow_id: SW:99, sibling_flags 80000040, crypto map: radius
        sa timing: remaining key lifetime (k/sec): (4237963/2229)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0x393783B6(959939510)
        transform: esp-aes esp-sha256-hmac ,
        in use settings ={Tunnel, }
        conn id: 100, flow_id: SW:100, sibling_flags 80000040, crypto map: radius
        sa timing: remaining key lifetime (k/sec): (4237970/2229)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)

     outbound ah sas:

     outbound pcp sas:
```

c) 다음 방법 중 하나를 사용하여 RADIUS 인증을 확인합니다.

- 8단계 (a)에서 생성한 사용자의 자격증명을 사용하여 네트워크 디바이스에 로그인합니다. RADIUS 인증 요청이 Cisco ISE 노드로 전송됩니다. **Live Authentications(**라이브 인증**)** 창에서 세부정보를 확인합니다.
- 엔드 호스트를 네트워크 디바이스에 연결하고 802.1X 인증을 구성합니다. 8단계 (a)에서 생성한 사용자의 자격증명을 사용하여 최종 호스트에 로그인합니다. RADIUS 인증 요청이 Cisco ISE 노드로 전송됩니다. **Live Authentications(**라이브 인증**)** 창에서 세부정보를 확인합니다.

ESR-5921에서 X.509 인증서 구성 및 설치

단계 **1** **esr** 명령을 입력하여 ESR 쉘(shell)을 시작합니다.

```
ise/admin# esr
% Entering ESR 5921 shell
% Cisco IOS Software, C5921 Software (C5921_I86-UNIVERSALK9-M), Version 15.5(2)T2, RELEASE SOFTWARE (fc3)
% Technical Support: http://www.cisco.com/techsupport
% Copyright (c) 1986-2015 Cisco Systems, Inc.

Press RETURN to get started, CTRL-C to exit

ise-esr5921>
ise-esr5921>
```

참고 FIPS 규정 준수를 위해 8자 이상의 비밀번호를 구성해야 합니다. **Enable secret level 1** 명령을 입력하여 비밀번호를 지정합니다.

```
ise-esr5921(config)#enable secret level 1 ?
0 Specifies an UNENCRYPTED password will follow
5 Specifies a MD5 HASHED secret will follow
8 Specifies a PBKDF2 HASHED secret will follow
9 Specifies a SCRYPT HASHED secret will follow
LINE The UNENCRYPTED (cleartext) 'enable' secret
```

참고 GUI에서 사용자 맞춤화된 RADIUS 포트(1645, 1646, 1812, 1813 이외)를 구성하는 경우 ESR 쉘(shell)에서 다음 CLI 명령을 입력하여 구성된 RADIUS 포트를 수락해야 합니다.

```
ip nat inside source static udp 10.1.1.2 [port_number] interface Ethernet0/0 [port_number]
```

단계 **2** 다음 명령을 사용하여 RSA 키 페어를 생성합니다.

예제:

```
crypto key generate rsa label rsa2048 exportable modulus 2048
```

단계 **3** 다음 명령을 사용하여 트러스트 포인트를 생성합니다.

예제:

```
crypto pki trustpoint trustpoint-name

enrollment terminal
serial-number none
fqdn none
ip-address none
subject-name cn=networkdevicename.cisco.com
revocation-check none
rsakeypair rsa2048
```

단계 **4** 다음 명령을 사용하여 인증서 서명 요청을 생성합니다.

예제:

```
crypto pki enroll rsaca-mytrustpoint

Display Certificate Request to terminal? [yes/no]: yes
```

단계 **5** 인증서 서명 요청의 출력을 텍스트 파일에 복사하고 서명을 위해 외부 CA에 제출하고 서명된 인증서 및 CA 인증서를 가져옵니다.

단계 **6** 다음 명령을 사용하여 CA(Certificate Authority) 인증서를 가져옵니다.

예제**:**

```
crypto pki authenticate rsaca-mytrustpoint
```

"—**BEGIN**—" 및 "—**-End**—" 줄을 포함하여 CA 인증서의 내용을 복사하여 붙여 넣습니다.

단계 **7** 다음 명령을 사용하여 서명된 인증서를 가져옵니다.

예제**:**

```
crypto pki import rsaca-mytrustpoint
```

"—**BEGIN**—" 및 "—**-End**—" 줄을 포함하여 서명된 인증서의 내용을 복사하여 붙여 넣습니다.

다음은 Cisco 5921 ESR에서 X.509 인증서를 구성하고 설치할 때 표시되는 출력의 예입니다.

```
ise-esr5921#show running-config
!
hostname ise-esr5921
!
boot-start-marker
boot host unix:default-config
boot-end-marker
!
no aaa new-model
bsd-client server url https://cloudsso.cisco.com/as/token.oauth2
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
call-home
! If contact email address in call-home is configured as sch-smart-licensing@cisco.com
! the email address configured in Cisco Smart License Portal will be used as contact email address to
send SCH notifications.
contact-email-addr sch-smart-licensing@cisco.com
profile "CiscoTAC-1"
  active
  destination transport-method http
  no destination transport-method email
!
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
crypto pki trustpoint SLA-TrustPoint
enrollment pkcs12
revocation-check crl
!
crypto pki trustpoint rsaca-mytrustpoint
enrollment terminal
serial-number none
fqdn none
ip-address none
subject-name cn=ise-5921.cisco.com
revocation-check none
rsakeypair rsa2048
!
crypto pki certificate chain SLA-TrustPoint
certificate ca 01
```

```
  30820321 30820209 A0030201 02020101 300D0609 2A864886 F70D0101 0B050030
  32310E30 0C060355 040A1305 43697363 6F312030 1E060355 04031317 43697363
  6F204C69 63656E73 696E6720 526F6F74 20434130 1E170D31 33303533 30313934
  3834375A 170D3338 30353330 31393438 34375A30 32310E30 0C060355 040A1305
  43697363 6F312030 1E060355 04031317 43697363 6F204C69 63656E73 696E6720
  526F6F74 20434130 82012230 0D06092A 864886F7 0D010101 05000382 010F0030
  82010A02 82010100 A6BCBD96 131E05F7 145EA72C 2CD686E6 17222EA1 F1EFF64D
  CBB4C798 212AA147 C655D8D7 9471380D 8711441E 1AAF071A 9CAE6388 8A38E520
  1C394D78 462EF239 C659F715 B98C0A59 5BBB5CBD 0CFEBEA3 700A8BF7 D8F256EE
  4AA4E80D DB6FD1C9 60B1FD18 FFC69C96 6FA68957 A2617DE7 104FDC5F EA2956AC
  7390A3EB 2B5436AD C847A2C5 DAB553EB 69A9A535 58E9F3E3 C0BD23CF 58BD7188
  68E69491 20F320E7 948E71D7 AE3BCC84 F10684C7 4BC8E00F 539BA42B 42C68BB7
  C7479096 B4CB2D62 EA2F505D C7B062A4 6811D95B E8250FC4 5D5D5FB8 8F27D191
  C55F0D76 61F9A4CD 3D992327 A8BB03BD 4E6D7069 7CBADF8B DF5F4368 95135E44
  DFC7C6CF 04DD7FD1 02030100 01A34230 40300E06 03551D0F 0101FF04 04030201
  06300F06 03551D13 0101FF04 05300301 01FF301D 0603551D 0E041604 1449DC85
  4B3D31E5 1B3E6A17 606AF333 3D3B4C73 E8300D06 092A8648 86F70D01 010B0500
  03820101 00507F24 D3932A66 86025D9F E838AE5C 6D4DF6B0 49631C78 240DA905
  604EDCDE FF4FED2B 77FC460E CD636FDB DD44681E 3A5673AB 9093D3B1 6C9E3D8B
  D98987BF E40CBD9E 1AECA0C2 2189BB5C 8FA85686 CD98B646 5575B146 8DFC66A8
  467A3DF4 4D565700 6ADF0F0D CF835015 3C04FF7C 21E878AC 11BA9CD2 55A9232C
  7CA7B7E6 C1AF74F6 152E99B7 B1FCF9BB E973DE7F 5BDDEB86 C71E3B49 1765308B
  5FB0DA06 B92AFE7F 494E8A9E 07B85737 F3A58BE1 1A48A229 C37C1E69 39F08678
  80DDCD16 D6BACECA EEBC7CF9 8428787B 35202CDC 60E4616A B623CDBD 230E3AFB
  418616A9 4093E049 4D10AB75 27E86F73 932E35B5 8862FDAE 0275156F 719BB2F0
  D697DF7F 28
        quit
crypto pki certificate chain rsaca-mytrustpoint
certificate 39
  30820386 3082026E A0030201 02020139 300D0609 2A864886 F70D0101 0B050030
  61310B30 09060355 04061302 5553310B 30090603 5504080C 024E4331 0C300A06
  03550407 0C035254 50310E30 0C060355 040A0C05 43495343 4F310C30 0A060355
  040B0C03 53544F31 19301706 03550403 0C107273 6163612E 65726368 616F2E63
  6F6D301E 170D3136 30393031 32313037 34335A17 0D313730 39303132 31303734
  335A301D 311B3019 06035504 03131269 73652D35 3932312E 63697363 6F2E636F
  6D308201 22300D06 092A8648 86F70D01 01010500 0382010F 00308201 0A028201
  0100EE87 CABFBA18 7E0405A8 ACAAAB23 E7CB6109 2CF98BAE 8EE93536 BF1EBBD3
  73E60BE7 F430B5AF EBF8B0C5 969B2828 A6783BB4 64E333E4 29C8744E 6E783617
  194AF1B0 7F04B4EA B89FD6EB F9C4F2DD 196DC6E0 CAA49B8B 665B6E0D 2FBC1D2F
  8E8181B9 60FAE126 D1B2E4E4 1F321A97 10C1B76A C2BB3174 361B13FA 2CB7BDFE
  22C0C33F 2792D714 C41E2237 00B1AE49 6593DCC3 A799D526 D81F9706 A71DA14E
  5ED76038 7A2C84B4 C668E35C 337BA1DC 9CA56AC2 C8E0059F 660CE39C 925310A0
  F9A21FFB 3C3C507A 20B924F7 E0125D60 6552321C 35736079 42449401 15E68DA6
  B4776DAA FB5AFDF8 59E31373 263175E3 1F14416A 24C21D69 A46173B6 96CC84FB
  5B9D0203 010001A3 818C3081 89300906 03551D13 04023000 302C0609 60864801
  86F84201 0D041F16 1D4F7065 6E53534C 2047656E 65726174 65642043 65727469
  66696361 7465301D 0603551D 0E041604 146DD31C 03690B98 330B67FA 6EDC7B20
  F99FB924 60301F06 03551D23 04183016 8014966A 0C21AF96 3E827690 423599CC
  EE8087A1 2909300E 0603551D 0F0101FF 04040302 05A0300D 06092A86 4886F70D
  01010B05 00038201 0100C0B9 D2845D97 6FFC16DB 01559659 BC1DECA6 E1A01965
  1F6CD459 E03D7ABE 91179FEB 08BF5B9B 84B62C36 236F528E E30C921C 81DA29E1
  EA3DFDC1 B0B0EEBA 14EADAEC 078576E4 D643A0EF 7D8E0880 C5FC3965 811B08C0
  5696DBF5 FADA4092 ACF549B8 2257F508 636D52AA 6CDC9596 AB43313F 6C33C9C1
  2CFDDBE3 EA9D407C 8D1B0F49 BBACD0CD 2832AC12 CD3FEFC8 501E1639 A4EFDC27
  69CA0147 971A1B2D DB2758E6 A84AFC86 4F9A4942 3D7EDBCC 7BDCC1BB 61F69B31
  BF13E39B 10AAC31C 55E73C8B C30BE516 7C506FF4 AC367D94 814A6880 EF201A6D
  CD2E1A95 7BBEC982 01CE867D 931F56E1 1EF1C457 9DC9A0BE 9DB2DC9B 19873585
  89AE82F6 A37E51D6 EECD
        quit
certificate ca 008DD3A81106B14664
  308203A2 3082028A A0030201 02020900 8DD3A811 06B14664 300D0609 2A864886
  F70D0101 05050030 61310B30 09060355 04061302 5553310B 30090603 5504080C
  024E4331 0C300A06 03550407 0C035254 50310E30 0C060355 040A0C05 43495343
  4F310C30 0A060355 040B0C03 53544F31 19301706 03550403 0C107273 6163612E
```

```
  65726368 616F2E63 6F6D301E 170D3135 31303231 32313135 34335A17 0D323531
  30313832 31313534 335A3061 310B3009 06035504 06130255 53310B30 09060355
  04080C02 4E43310C 300A0603 5504070C 03525450 310E300C 06035504 0A0C0543
  4953434F 310C300A 06035504 0B0C0353 544F3119 30170603 5504030C 10727361
  63612E65 72636861 6F2E636F 6D308201 22300D06 092A8648 86F70D01 01010500
  0382010F 00308201 0A028201 0100CB82 2AECEE38 1BCB27B9 FA5F2FBD 8609B190
  16A6F741 5BEC18B8 8B260CAF 190EA1CE 063BC558 556DC085 6FAC5425 14AFE225
  0E9E3A12 05F3DA7E D17E03F2 7FFE92FB 38D67027 DBC5C175 EB53E96B 66C20D11
  B4C32D38 AE04385C 8FD4CB74 31A97824 CA1CAFD5 091806C3 6F9CBF8D DC42DD5B
  D985703D F3BB9ED1 7DE99614 422D765C 86AB25CD E80008C5 22049BE8 66D1CA27
  E1EB6D4F 4FD3CC18 E091BBF0 6FE0EB52 B33F231A 6D6B7190 4196C929 D22E2C42
  B9CD2BBD 24550E82 8CD8838F C41B4DAD 2FA1636A 5787BBB2 F21E4718 335B005B
  DFBE6EA7 56EBE30B D52DE85F FFAF0189 E372CBFC 44BFF235 4DA7C9EF DAAC6D0A
  A196DA5A 1B525175 C26B3581 EA4B0203 010001A3 5D305B30 1D060355 1D0E0416
  0414966A 0C21AF96 3E827690 423599CC EE8087A1 2909301F 0603551D 23041830
  16801496 6A0C21AF 963E8276 90423599 CCEE8087 A1290930 0C060355 1D130405
  30030101 FF300B06 03551D0F 04040302 02A4300D 06092A86 4886F70D 01010505
  00038201 01002334 A3F0E5D3 4D229985 67A07754 73EC52E3 05B7D05F 926CC863
  220F849B 861C36B2 EF7C3485 474D4EF0 73895879 CAE08BBB 183B7CFA A20C4354
  86C6D9DF D445DACE C252C608 236F6673 F3F3C329 474B22E8 660BF91E 41054B8D
  43B80E44 AE69C164 2C9F41A2 8284F577 21FFAB8E A6771A5E DD34EBE4 A0DC2EAD
  95702010 02964566 478DA90F 5E134643 81A5F5EA 362D0394 1F9F23D1 DEE50B07
  12938299 1AF11A36 82DAFC6A 164B2F66 8B0AB7CC 9A723EBC B50E740B 0A9270E3
  60E2ED42 7F10D1A6 F6735144 AE93BF86 3D5A0502 6811D2BD 6E694693 28DE84C5
  3747CF0A D2B8D6C9 6CBEBA0A D1137CF8 E31CBF6B 437D82DD D74A4A9F 3557B3D9
  D0BD055F 65A8
        quit
license udi pid CISCO5921-K9 sn 9XG4481W768
username lab password 0 lab
!
redundancy
!
crypto keyring MVPN-spokes
rsa-pubkey address 0.0.0.0
  address 0.0.0.0
  key-string
  quit
!
crypto isakmp policy 10
encr aes
hash sha256
group 16
!
crypto isakmp policy 20
encr aes
hash sha256
group 14
crypto isakmp profile MVPN-profile
   description LAN-to-LAN for spoke router(s) connection
   keyring MVPN-spokes
   match identity address 0.0.0.0
!
crypto ipsec transform-set radius esp-aes esp-sha256-hmac
mode tunnel
crypto ipsec transform-set radius-2 esp-aes esp-sha256-hmac
mode transport
!
crypto dynamic-map MVPN-dynmap 10
set transform-set radius radius-2
!
crypto map radius 10 ipsec-isakmp dynamic MVPN-dynmap
!
interface Ethernet0/0
description e0/0->connection to external NAD
```

```
ip address 192.168.20.1 255.255.255.0
ip nat outside
ip virtual-reassembly in
no ip route-cache
crypto map radius
!
interface Ethernet0/1
description e0/1->tap0 internal connection to ISE
ip address 10.1.1.1 255.255.255.252
ip nat inside
ip virtual-reassembly in
no ip route-cache
!
interface Ethernet0/2
no ip address
shutdown
!
interface Ethernet0/3
no ip address
shutdown
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
ip nat inside source list 1 interface Ethernet0/0 overload
ip nat inside source static udp 10.1.1.2 1645 interface Ethernet0/0 1645
ip nat inside source static udp 10.1.1.2 1646 interface Ethernet0/0 1646
ip nat inside source static udp 10.1.1.2 1812 interface Ethernet0/0 1812
ip nat inside source static udp 10.1.1.2 1813 interface Ethernet0/0 1813
!
access-list 1 permit 10.1.1.0 0.0.0.3
!
control-plane
!
line con 0
logging synchronous
line aux 0
line vty 0 4
login
transport input none
!
end
```

다음은 Cisco Catalyst 3850 시리즈 스위치에서 X.509 인증서를 구성하고 설치할 때 표시되는 출력의 예입니다.

```
cat3850#show running-config

enable password lab
!
username lab password 0 lab
aaa new-model

!

aaa group server radius ise
server name ise-vm
deadtime 60
!
aaa authentication login default group radius local

aaa authentication enable default group radius enable

!
```

```
crypto isakmp policy 10

encr aes

hash sha256
authentication rsa-sig
group 16
!
crypto ipsec security-association lifetime seconds 86400
!
crypto ipsec transform-set radius esp-aes esp-sha256-hmac
mode tunnel

!

crypto ipsec profile radius-profile

!

crypto map radius 10 ipsec-isakmp
set peer 192.168.20.1
set transform-set radius

match address 100

!

interface GigabitEthernet1/0/1
no switchport
ip address 192.168.20.2 255.255.255.0

crypto map radius

!
access-list 100 permit ip host 192.168.20.2 host 192.168.20.1
!
snmp-server community public RO
snmp-server community private RW
!
radius server rad-ise
address ipv4 192.168.20.1 auth-port 1645 acct-port 1646

key secret
```

예: Cisco Catalyst 3850 Series 스위치의 사전 공유 키 컨피그레이션 출력

다음은 Cisco Catalyst 3850 Series 스위치에서 사전 공유 키를 구성할 때 표시되는 출력의 예입니다.

```
cat3850#show running-config

enable password lab
 !
 username lab password 0 lab
 aaa new-model
 !
 aaa group server radius ise
 server name ise-vm
 deadtime 60
 !
 aaa authentication login default group radius local
```

```
 aaa authentication enable default group radius enable

!

crypto isakmp policy 10

 encr aes

 hash sha256
 authentication pre-share
 group 16
 crypto isakmp key 123456789 address 0.0.0.0
 !
 crypto ipsec security-association lifetime seconds 86400
 !
 crypto ipsec transform-set radius esp-aes esp-sha256-hmac
 mode tunnel
 !
 crypto ipsec profile radius-profile
 !
 crypto map radius 10 ipsec-isakmp
 set peer 192.168.20.1
 set transform-set radius
 match address 100
!
interface GigabitEthernet1/0/1
 no switchport
 ip address 192.168.20.2 255.255.255.0

 crypto map radius
!
 access-list 100 permit ip host 192.168.20.2 host 192.168.20.1
 !
 snmp-server community public RO
 snmp-server community private RW
 !
 radius server rad-ise
 address ipv4 192.168.20.1 auth-port 1645 acct-port 1646

 key secret
```

Mobile Device Manager와 Cisco ISE와 상호운용성

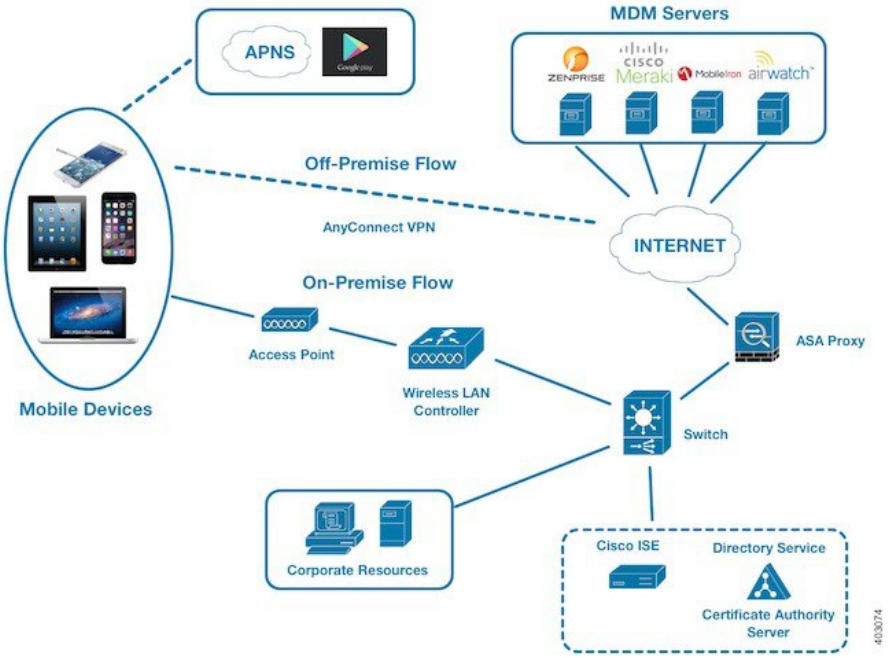
MDM(Mobile Device Management) 서버는 모바일 운영자, 서비스 제공자 및 엔터프라이즈 전반에 걸쳐 구축된 모바일 디바이스를 보호, 모니터링, 관리 및 지원합니다. MDM 서버는 구축된 환경의 모바일 디바이스에 있는 일부 애플리케이션(예: 이메일 애플리케이션)의 사용을 제어하는 정책 서버로 작동합니다. 그러나 네트워크는 ACL(액세스 제어 목록)을 기반으로 엔드포인트에 대한 세부적인 액세스를 제공할 수 있는 유일한 엔티티입니다. Cisco ISE는 MDM 서버에 필요한 디바이스 속성을 쿼리하여 그러한 디바이스에 대한 네트워크 액세스 제어를 제공하는 ACL을 생성합니다.

여러 벤더의 MDM 서버를 비롯하여 여러 활성 MDM 서버를 네트워크에서 실행할 수 있습니다. 이렇게 하면 위치 또는 디바이스 유형과 같은 디바이스 요소를 기반으로 MDM 서버마다 각기 다른 엔드포인트를 라우팅할 수 있습니다.

Cisco ISE는 또한 디바이스에서 Cisco AnyConnect 4.1 및 Cisco Adaptive Security Appliances 9.3.2 이상 버전을 사용하여 VPN을 통해 네트워크에 액세스할 수 있도록 Cisco MDM Server Info API, 버전 2를 사용하여 MDM 서버와 통합됩니다.

다음 그림에서 Cisco ISE는 시행 포인트이고 MDM 정책 서버는 정책 정보 포인트입니다. Cisco ISE는 MDM 서버에서 데이터를 가져와 완벽한 솔루션을 제공합니다.

그림 ***3: Cisco ISE***와의 ***MDM*** 상호운용성



하나 이상의 외부 MDM(Mobile Device Manager) 서버와 상호운용되도록 Cisco ISE를 구성할 수 있습니다. 이 유형의 타사 연결을 설정하면 MDM 데이터베이스에서 사용 가능한 자세한 정보를 활용할 수 있습니다. Cisco ISE에서는 REST API 호출을 사용하여 외부 MDM 서버에서 정보를 가져옵니다. Cisco ISE에서는 스위치, 액세스 라우터, 무선 액세스 포인트 및 다른 네트워크 액세스 포인트에 적절한 액세스 제어 정책을 적용합니다. 이 정책을 통해 Cisco ISE 지원 네트워크에 액세스하는 원격 디바이스를 보다 효과적으로 제어할 수 있습니다.

Cisco ISE에서 지원하는 MDM 벤더 목록은 지원되는 모바일 디바이스 관리 서버, 58 페이지를 참조하십시오.

지원되는 모바일 디바이스 관리 활용 사례

Cisco ISE는 외부 MDM 서버를 이용해 다음과 같은 기능을 수행합니다.

- 디바이스 등록 관리: 네트워크에 액세스하는 등록되지 않은 엔드포인트는 MDM 서버에서 호스팅되는 등록 페이지로 리디렉션됩니다. 디바이스 등록에는 사용자 역할, 디바이스 유형 등이 포함됩니다.
- 디바이스 교정 처리: 교정 중 제한된 액세스 권한만 엔드포인트에 부여됩니다.

- 엔드포인트 데이터 보완: Cisco ISE 프로파일링 서비스를 사용하여 수집할 수 없는 MDM 서버의 정보로 엔드포인트 데이터베이스를 업데이트합니다. Cisco ISE는 **Endpoints(**엔드포인트**)** 창에서 볼 수있는 6가지 디바이스 속성을 사용합니다. Cisco ISE GUI에서 **Menu(**메뉴**)** 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Network Access(**네트워크 액세스**)** > **Identities(ID)** > **Endpoints(**엔드포인트**)**를 선택합니다.

  다음은 사용 가능한 디바이스 속성의 예입니다.

- MDMImei: 99 000100 160803 3
- MDMManufacturer: Apple
- MDMModel: iPhone
- MDMOSVersion: iOS 6.0.0
- MDMPhoneNumber: 9783148806
- MDMSerialNumber: DNPGQZGUDTF9

- 4시간마다 MDM 서버를 폴링하여 디바이스 규정 준수 데이터를 확인합니다. **External MDM Servers(**외부 **MDM** 서버**)** 창에서 폴링 간격을 구성합니다. (이 창을 보려면 **Menu(**메뉴**)** 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Network Access(**네트워크 액세스**)** > **Network Resources(**네트워크 리소스**)** > **Network Resources(**외부 **MDM** 서버**)**를 선택합니다.
- MDM 서버를 통해 디바이스 명령 실행: Cisco ISE가 MDM 서버를 통해 사용자 디바이스에 대한 원격 작업을 발급합니다. **Endpoints(**엔드포인트**)** 창을 통해 Cisco ISE 관리 포털에서 원격 작업을 시작합니다. 이 창을 보려면 **Menu(**메뉴**)** 아이콘(☰)을 클릭하고 **Context Visibility Endpoints(**상황 가시성 엔드포인트**)** > **Endpoints(**엔드포인트**)**를 선택합니다. MDM 서버 옆의 확인란을 선택하고 **MDM Actions(MDM** 작업**)**를 클릭합니다. 표시되는 드롭다운 목록에서 필요한 작업을 선택합니다.

벤더 **MDM** 속성

Cisco ISE에서 MDM 서버를 구성하면 Cisco ISE 시스템 사전에 **mdm**이라는 이름의 새 항목에 벤더의 속성이 추가됩니다. 다음 속성은 등록 상태에 사용되며 일반적으로 MDM 벤더에서 지원합니다.

- DeviceRegisterStatus
- DeviceCompliantStatus
- DiskEncryptionStatus
- PinLockStatus
- JailBrokenStatus
- Manufacturer
- IMEI

- SerialNumber
- OsVersion
- PhoneNumber
- MDMServerName
- MDMServerReachable
- MEID
- Model
- UDID

벤더의 고유한 속성이 지원되지 않는 경우 ERS API를 사용하여 벤더별 속성을 교환할 수 있습니다. 지원되는 ERS API에 대한 자세한 내용은 벤더의 설명서를 참조합니다.

권한 부여 정책에 사용 가능한 새 MDM 사전 속성을 확인할 수 있습니다.

지원되는 모바일 디바이스 관리 서버

지원되는 MDM 서버에는 다음 벤더의 제품이 포함됩니다.

- Absolute
- Blackberry - BES
- Blackberry - Good Secure EMM
- Cisco0 Meraki Systems Manager
- Citrix Endpoint Management(이전 명칭: Xenmobile)
- Globo
- IBM MaaS360
- JAMF Casper Suite
- Microsoft Intune(모바일 디바이스용)
- Microsoft SCCM(데스크톱 디바이스용)
- MobileIron UEM

참고 일부 MobileIron 버전은 Cisco ISE에서 작동하지 않습니다. MobileIron에서 이 문제를 인지하고 있으며 해결 방법을 마련했습니다. 자세한 내용은 MobileIron에 문의하십시오.

- Mosyle

- SAP Afaria
- Sophos
- SOTI MobiControl
- Symantec
- Tangoe
- VMware Workspace ONE(이전 명칭: AirWatch)
- 42 Gears

ISE 커뮤니티 리소스

How To: Meraki EMM / MDM Integration with ISE

모바일 디바이스 관리 서버에서 사용하는 포트

다음 표에는 Cisco ISE와 MDM 서버가 서로 통신할 수 있도록 하려면 열어야 하는 포트가 나와 있습니다. MDM 에이전트와 서버에서 열어야 하는 포트의 목록은 MDM 벤더 설명서를 참고해 주십시오.

표 ***15: MDM*** 서버에서 사용되는 포트

MDM 서버	포트
MobileIron	443
Zenprise	443
Good	19005
Airwatch	443
Afaria	443
Fiberlink MaaS	443
Meraki	443
Microsoft Intune	80 및 443
Microsoft SCCM	80 및 443

모바일 디바이스 관리 통합 프로세스 플로우

1. 사용자가 SSID를 사용하여 디바이스를 연결합니다.
2. Cisco ISE에서 MDM 서버에 대한 API 호출을 수행합니다.
3. 이 API 호출에서는 사용자의 디바이스 목록 및 디바이스의 포스처 상태가 반환됩니다.

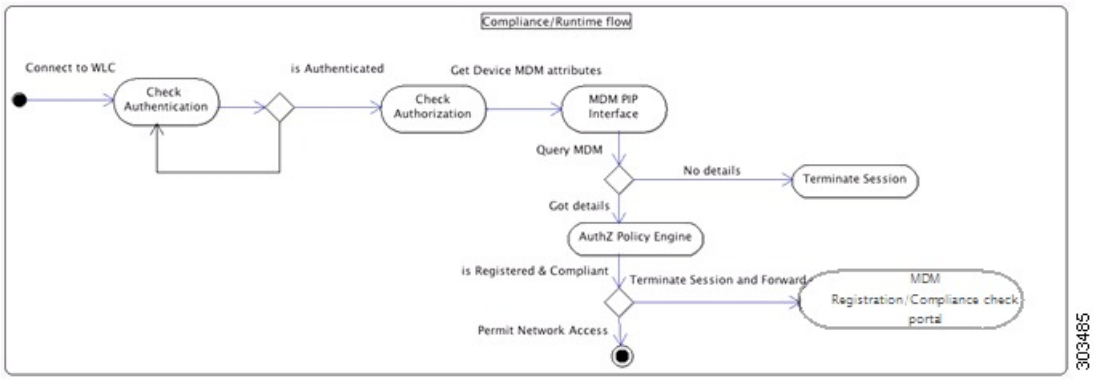
참고 입력 매개변수는 엔드포인트 디바이스의 MAC 주소입니다. 오프프레미스 Apple iOS 디바이스(VPN을 통해 Cisco ISE에 연결하는 모든 디바이스)의 경우 입력 매개변수는 UDID입니다.

4. 이 목록에 없는 사용자 디바이스는 등록되지 않은 것입니다. Cisco ISE가 Cisco ISE로의 리디렉션을 위한 권한 부여 요청을 NAD에 보냅니다. 그러면 사용자에게 MDM 서버 페이지가 표시됩니다.

참고 MDM 포털을 통해 Cisco ISE 네트워크 외부의 MDM 서버에 등록된 디바이스를 등록해야 합니다. 이는 Cisco ISE 릴리스 1.4 이상에 적용됩니다. 이전 Cisco ISE 버전에서는 Cisco ISE 지원 네트워크 외부에 등록된 디바이스가 포스처 정책을 준수하는 경우 자동으로 등록될 수 있습니다.

5. Cisco ISE가 MDM을 사용하여 디바이스를 프로비저닝하고 사용자가 디바이스를 등록할 수 있는 적절한 창을 표시합니다.
6. 사용자가 MDM 서버에서 디바이스를 등록합니다. 그러면 MDM 서버가 자동 리디렉션 또는 수동 브라우저 새로 고침을 통해 요청을 Cisco ISE로 리디렉션합니다.
7. Cisco ISE가 MDM 서버를 다시 쿼리하여 포스처 상태를 확인합니다.
8. 사용자 디바이스가 MDM 서버에 구성되어 있는 포스처(규정 준수) 정책을 준수하지 않으면 디바이스가 규정을 준수하지 않는다는 알림이 사용자에게 표시됩니다. 사용자는 디바이스가 규정을 준수하도록 필요한 조치를 취해야 합니다.
9. 사용자 디바이스가 규정을 준수하면 MDM 서버가 내부 표에서 디바이스 상태를 업데이트합니다.
10. 사용자가 지금 브라우저를 새로 고치면 제어권이 Cisco ISE로 다시 전송됩니다.
11. Cisco ISE가 4시간마다 MDM 서버를 폴링하여 규정 준수 정보를 가져오고 적절한 CoA(Change of Authorization)를 발급합니다. 폴링 간격을 구성할 수 있습니다. 또한 Cisco ISE는 MDM 서버가 사용 가능한 상태인지를 5분마다 확인합니다.

다음 그림에는 MDM 프로세스 플로우이 나와 있습니다.



참고 각 디바이스는 한 번에 하나의 MDM 서버에만 등록할 수 있습니다. 다른 벤더의 MDM 서비스에 동일한 디바이스를 등록하려는 경우에는 이전 벤더의 프로파일을 디바이스에서 제거해야 합니다. MDM 서비스는 대개 "회사 초기화" 기능을 제공합니다. 이 기능은 디바이스(전체 디바이스 아님)의 벤더 컨피그레이션만 삭제합니다. 사용자가 파일을 제거할 수도 있습니다. 예를 들어 사용자는 iOS 디바이스에서 Settings(설정) > General(일반) >Device management(디바이스 관리) 창으로 이동하여 **Remove management(**제거 관리**)**를 클릭할 수 있습니다. 또는 사용자가 ISE에서 내 디바이스 포털로 이동하여 **Corporate Wipe(**회사 초기화**)**를 클릭할 수도 있습니다.

Cisco ISE를 통한 모바일 디바이스 관리 서버 설정

Cisco ISE를 사용하여 MDM 서버를 설정하려면 다음과 같은 높은 수준의 작업을 수행해야 합니다.

단계 **1** MDM 서버 인증서를 Cisco ISE로 가져옵니다. 단, Intune의 경우에는 PAN(Policy Administration Node)의 인증서를 Azure로 가져옵니다.

단계 **2** Mobile Device Manager 정의를 생성합니다.

단계 **3** Wireless LAN Controller에서 ACL을 구성합니다.

단계 **4** 등록되지 않은 디바이스를 MDM 서버로 리디렉션하는 권한 부여 프로파일을 구성합니다.

단계 **5** 네트워크에 여러 MDM 서버가 있는 경우 각 벤더에 대해 별도의 권한 부여 프로파일을 구성합니다.

단계 **6** MDM 활용 사례용으로 권한 부여 정책 규칙을 구성합니다.

Cisco ISE로 모바일 디바이스 관리 서버 인증서 가져오기

Cisco ISE가 MDM 서버와 연결할 수 있도록 하려면 MDM 서버 인증서를 Cisco ISE 신뢰할 수 있는 인증서 저장소로 가져와야 합니다. MDDM 서버에 CA가 서명한 인증서가 있는 경우에는 루트 인증서를 Cisco ISE 신뢰할 수 있는 인증서 저장소로 가져와야 합니다.

참고 Microsoft Azure의 경우 Cisco ISE 인증서를 Azure로 가져옵니다. 모바일 디바이스 관리 서버로 Microsoft Intune을 Cisco ISE에 연결, 65 페이지의 내용을 참조하십시오.

단계 **1** MDM 서버에서 MDM 서버 인증서를 내보낸 다음 로컬 머신에 저장합니다.

단계 **2** Cisco ISE GUI에서 **Menu(**메뉴**)** 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Certificates(**인증서**)** > **Trusted Certificate(**신뢰할 수 있는 인증서**)** > **Import(**가져오기**)**를 선택합니다.

단계 **3** **Import a new Certificate into the Certificate Store(**인증서 저장소로 새 인증서 가져오기**)** 창에서 **Choose File(**파일 선택**)**을 클릭하여 MDM 서버에서 가져온 MDM 서버 인증서를 선택합니다.

단계 4 **Friendly Name(**식별 이름**)** 필드에 인증서의 이름을 입력합니다.

단계 5 **Trust for authentication within ISE(ISE** 내의 인증 신뢰**)** 확인란을 선택합니다.

단계 6 **Submit(**제출**)**을 클릭합니다.

단계 7 **Trust Certificates(**신뢰 인증서**)** 창에 새로 추가된 MDM 서버 인증서가 나열되어 있는지 확인합니다.

다음에 수행할 작업

Cisco ISE에서 디바이스 관리 서버 정의, 62 페이지

에 전달하는 고성능 고속 어플라이언스입니다.

Cisco ISE에서 디바이스 관리 서버 정의

Cisco ISE가 필요한 서버와 통신할 수 있도록 Cisco ISE에서 모바일 및 데스크톱 디바이스 관리 서버를 정의합니다. 서버와의 통신에 사용되는 인증 유형, Cisco ISE가 디바이스 관리 서버에서 디바이스 정보를 요청하는 빈도 등을 구성할 수 있습니다.

모바일 관리 서버를 정의하려면 Cisco ISE에서 모바일 디바이스 관리 서버 정의, 62 페이지의 내용을 참조하십시오.

Microsoft SCCM(System Center Configuration Manager) 서버를 정의하려면 데스크톱 디바이스 관리자 서버에서 엔드포인트 규정 준수에 대한 구성 베이스라인 정책 선택를 참조하십시오.

Cisco ISE에서 모바일 디바이스 관리 서버 정의

단계 1 Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Network Resources(**네트워크 리소스**)** > **External MDM(**외부 **MDM)**

단계 2 **MDM Servers(MDM** 서버**)** 창에서 를 클릭합니다.

단계 3 추가할 MDM 서버의 이름과 설명을 해당 필드에 입력합니다.

단계 4 **Server Type(**서버 유형**)** 드롭 다운 목록에서 **Mobile Device Manager(**모바일 디바이스 관리자**)**를 선택합니다.

단계 5 **Authentication Type(**인증 유형**)** 드롭다운 목록에서 **Basic(**기본**)** 또는 **OAuth - Client Credentials(OAuth -** 클라이언트 자격 증명**)**을 선택합니다.

Basic(기본**)** 인증 유형을 선택하면 다음 필드가 표시됩니다.

- **Host Name / IP Address(**호스트 이름**/IP** 주소**)**: MDM 서버의 호스트 이름 또는 IP 주소를 입력합니다.
- **Port(**포트**)**: MDM 서버에 연결할 때 사용할 포트(일반적으로 443)를 입력합니다,
- **Instance Name(**인스턴스 이름**)**: 이 MDM 서버에 인스턴스가 여러 개 있는 경우 연결하려는 인스턴스를 입력합니다.
- **Username(**사용자 이름**)**: MDM 서버에 연결하는 데 사용해야 하는 사용자 이름을 입력합니다.
- **Password(**비밀번호**)**: MDM 서버에 연결하는 데 사용할 비밀번호를 입력합니다.

- **Polling Interval(**폴링 간격**)**: Cisco ISE가 규정 준수 확인 정보를 위해 MDM 서버를 폴링할 폴링 간격을 분 단위로 입력합니다. 이 값은 MDM 서버의 폴링 간격과 동일해야 합니다. 유효 범위는 15분~1440분입니다. 기본값은 240분입니다. 네트워크의 활성 클라이언트 몇 개를 테스트할 경우 폴링 간격을 60분 미만으로 설정하는 것이 좋습니다. 활성 클라이언트가 많은 프로덕션 환경에서 이 값을 60분 미만으로 설정하면 시스템의 로드가 크게 증가하여 성능이 저하될 수 있습니다.

  폴링 간격을 0으로 설정하면 Cisco ISE는 MDM 서버와의 통신을 비활성화합니다.

- **Time Interval For Compliance Device ReAuth Query(**규정 준수 디바이스 재인증 쿼리 시간 간격**)**: 엔드포인트가 인증되거나 재인증되는 경우 Cisco ISE는 캐시를 사용하여 해당 엔드포인트에 대한 MDM 변수를 가져옵니다. 캐시된 값의 기간이 이 필드에 구성된 값보다 높은 경우 Cisco ISE는 새 디바이스 쿼리를 MDM 서버로 보내 새 값을 가져옵니다. 규정 준수 상태가 변경된 경우 Cisco ISE는 적절한 CoA를 트리거합니다.

  유효 범위는 1분~1440분입니다. 기본값은 1분입니다.

OAuth - Client Credentials(클라이언트 자격 증명**)** 인증 유형을 선택하면 다음 필드가 표시됩니다.

- **Auto Discovery(**자동 검색**)** 드롭다운 목록에서 **Yes(**예**)** 또는 **No(**아니요**)**를 선택합니다.

- **Auto Discovery URL(**자동 검색 **URL)**: Microsoft Azure 관리 포털에서 *Microsoft Azure AD Graph API* 엔드포인트의 값을 입력합니다. 이 URL은 애플리케이션이 Graph API를 사용하여 Microsoft Azure AD 디렉토리 내의 디렉토리 데이터에 액세스할 수 있는 엔드포인트입니다. URL 형식은 `https://<hostname>/<tenant id>`입니다.

  예를 들어 `https://graph.windows.net/47f09275-5bc0-4807-8aae-f35cb0341329`가 될 수 있습니다.

  이 URL을 펼친 버전은 `https://<Graph_API_Endpoint>/<TenantId_Or_Domain>/servicePrincipalsByAppId/<Microsoft Intune AppId>/serviceEndpoints?api-version=1.6&client-request-id=<Guid.NewGuid()>`와 같은 형식의 속성 파일에도 있습니다.

- **Client ID(**클라이언트 **ID)**: 애플리케이션의 고유 식별자입니다. 애플리케이션이 Microsoft Azure AD Graph API, Microsoft Intune API 등 다른 애플리케이션의 데이터에 액세스하는 경우 이 속성을 사용합니다.

- **Token Issuing URL(**토큰 발급 **URL)**: 이전 단계의 *Oauth2.0 Authorization Endpoint(Oauth2.0* 권한 부여 엔드포인트*)* 값을 입력합니다. 이 엔드포인트에서 앱이 OAuth2.0을 사용하여 액세스 토큰을 얻습니다. 앱이 인증되고 나면 Microsoft Azure AD는 앱(Cisco ISE)에 액세스 토큰을 발급합니다. 그러면 앱이 Graph API 또는Intune API를 호출할 수 있습니다.

- **Token Audience(**토큰 대상**)**: 토큰의 사용 대상인 수신자 리소스로, Microsoft Intune API에 대한 알려진 공용 **(APP ID URL)**앱 **ID URL**입니다.

- **Polling Interval(**폴링 간격**)**: Cisco ISE가 규정 준수 확인 정보를 위해 MDM 서버를 폴링할 폴링 간격을 분 단위로 입력합니다. 이 값은 MDM 서버의 폴링 간격과 동일해야 합니다. 유효 범위는 15분~1440분입니다. 기본값은 240분입니다. 네트워크의 활성 클라이언트 몇 개를 테스트할 경우 폴링 간격을 60분 미만으로 설정하는 것이 좋습니다. 활성 클라이언트가 많은 프로덕션 환경에서 이 값을 60분 미만으로 설정하면 시스템의 로드가 크게 증가하여 성능이 저하될 수 있습니다.

  폴링 간격을 0으로 설정하면 Cisco ISE는 MDM 서버와의 통신을 비활성화합니다.

- **Time Interval For Compliance Device ReAuth Query(**규정 준수 디바이스 재인증 쿼리 시간 간격**)**: 엔드포인트가 인증되거나 재인증되는 경우 Cisco ISE는 캐시를 사용하여 해당 엔드포인트에 대한 MDM 변수를 가져옵니

다. 캐시된 값의 기간이 이 필드에 구성된 값보다 높은 경우 Cisco ISE는 새 디바이스 쿼리를 MDM 서버로 보내 새 값을 가져옵니다. 규정 준수 상태가 변경된 경우 Cisco ISE는 적절한 CoA를 트리거합니다.

유효 범위는 1분~1440분입니다. 기본값은 1분입니다.

단계 **6** **Status(**상태**)** 드롭다운 목록에서 **Enabled(**활성화됨**)**를 선택합니다.

단계 **7** MDM 서버가 Cisco ISE에 연결되어 있는지 확인하려면 **Test Connection(**연결 테스트**)**을 클릭합니다. **Test Connection(**테스트 연결**)**은 모든 활용 사례(베이스 라인 가져 오기, 디바이스 정보 가져 오기 등)에 대한 권한을 확인하기 위한 것이 아닙니다. 이들은 서버가 Cisco ISE에 추가될 때 검증됩니다.

단계 **8** **Save(**저장**)**를 클릭합니다.

Microsoft Intune 및 Microsoft System Center Configuration Manager에 대한 Cisco ISE 모바일 디바이스 관리 지원

- **Microsoft Intune**: Cisco ISE는 모바일 디바이스를 관리하는 파트너 MDM 서버로 Microsoft Intune 디바이스 관리를 지원합니다.

  모바일 디바이스를 관리하는 Microsoft Intune 서버에서 Cisco ISE를 OAuth 2.0 클라이언트 애플리케이션으로 구성합니다. Cisco ISE는 Azure에서 토큰을 가져와 해당 Cisco ISE Intune 애플리케이션과 세션을 설정합니다.

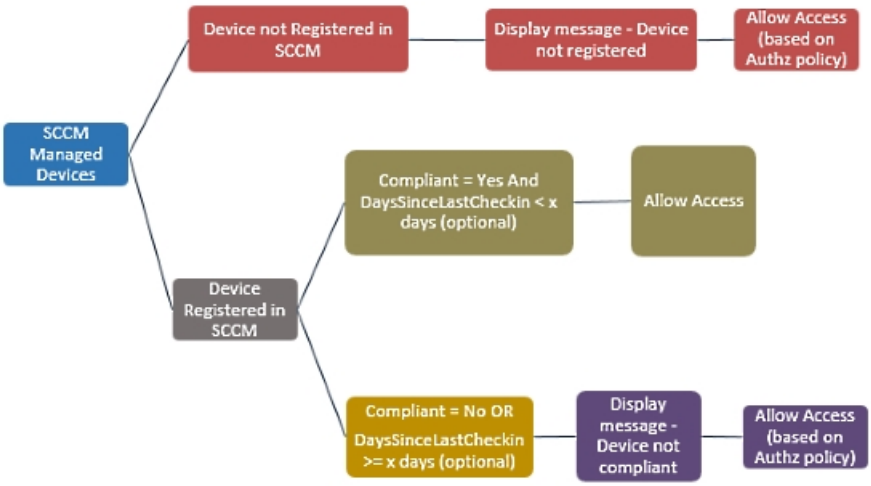
  Microsoft Intune이 클라이언트 애플리케이션과 통신하는 방법에 대한 자세한 내용은 https://msdn.microsoft.com/en-us/library/azure/dn645543.aspx를 참고하십시오.

- 데스크톱 디바이스 관리자**(Microsoft SCCM)**: Cisco ISE는 Windows 컴퓨터를 관리하는 파트너 MDM 서버로 Microsoft SCCM(System Center Configuration Manager)을 지원합니다. ISE는 WMI를 사용하여 SCCM 서버에서 규정 준수 정보를 검색하며 해당 정보를 사용하여 사용자의 Windows 디바이스에 대한 네트워크 액세스 권한을 부여하거나 거부합니다.

Microsoft SCCM 워크플로우

Cisco ISE는 디바이스 등록 여부 및 디바이스가 등록된 경우 규정 준수 여부에 대해 Microsoft SCCM 서버에서 정보를 검색할 수 있습니다. 다음 다이어그램에는 Microsoft SCCM에서 관리하는 디바이스의 워크플로우가 나와 있습니다.

그림 ***4: SCCM*** 워크플로우



디바이스가 네트워크에 연결되고 Microsoft SCCM 정책이 일치하면 Cisco ISE는 권한 부여 정책에 지정된 SCCM 서버를 쿼리하여 규정 준수 및 마지막 로그인(체크인) 시간을 검색합니다. 이 정보를 사용해 Cisco ISE는 **Endpoint(**엔드포인트**)** 목록에서 디바이스의 규정 준수 상태 및 lastCheckinTimeStamp를 업데이트합니다.

디바이스가 규정을 준수하지 않거나 Microsoft SCCM에 등록되어 있지 않으며 권한 부여 정책에서 리디렉션 프로파일이 사용되는 경우에는 디바이스가 규정을 준수하지 않거나 Microsoft SCCM에 등록되어 있지 않다는 메시지가 사용자에게 표시됩니다. 사용자가 메시지를 확인하고 나면 Cisco ISE는 Microsoft SCCM 등록 사이트에 CoA를 실행할 수 있습니다. 권한 부여 정책과 프로파일에 따라 사용자에게 액세스 권한이 부여됩니다.

Microsoft SCCM 서버 연결 모니터링

Microsoft SCCM에 대한 폴링 간격을 구성할 수 없습니다.

Cisco ISE는 Microsoft SCCM 서버 연결을 확인하는 MDM 하트비트 작업을 실행하며 Microsoft SCCM 서버 연결이 끊기면 경보를 생성합니다. 하트비트 작업 간격은 구성할 수 없습니다.

모바일 디바이스 관리 서버로 **Microsoft Intune**을 **Cisco ISE**에 연결

단계 **1** Microsoft Azure 포털에 로그인하고 **Active Directory**를 선택합니다.

단계 **2** **New Registration(**새 등록**)**을 클릭합니다.

단계 **3** 표시되는 **Register An Application(**애플리케이션 등록**)** 창에서 **Name(**이름**)** 필드에 값을 입력합니다.

단계 **4** **Supported Account Types(**지원되는 계정 유형**)** 영역에서 **Accounts in this organizational directory only(**이 조직 디렉토리에 있는 계정만**)** 라디오 버튼을 클릭합니다.

단계 **5** **Register(**등록**)**를 클릭합니다.

단계 **6** 새로 등록된 애플리케이션의 **Overview(**개요**)** 창이 표시됩니다. 이 창이 열린 상태에서 Cisco ISE 관리 포털에 로그인합니다.

단계 **7** Cisco ISE GUI에서 **Menu(**메뉴**)** 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Certificates(**인증서**)** > **System(**시스템**)** > **Certificates(**인증서**)**를 선택합니다.

단계 **8** 표시된 인증서 목록에서 기본 자가서명 서버 인증서 또는 관리자 사용을 위해 구성한 다른 인증서를 선택합니다. 원하는 인증서의 확인란을 선택합니다.

단계 **9** **Export(**내보내기**)**를 클릭합니다.

단계 **10** 표시되는 대화 상자에서 **Export Certificate Only(**인증서만 내보내기**)** 라디오 버튼을 클릭하고 **Export(**내보내기**)**를 클릭합니다.

단계 **11** 해당 인증서의 세부정보를 보려면 **View(**보기**)**를 클릭합니다. 표시된 **Certificate Hierarchy(**인증서 계층 구조**)** 대화 상자를 아래로 스크롤하여 **Fingerprints(**핑거프린트**)** 영역으로 이동합니다. 이후 단계에서 해당 값을 참조하게 됩니다.

단계 **12** Microsoft Azure Active Directory 포털의 왼쪽 메뉴 패널에서 **Certificates and Secrets(**인증서 및 암호**)**를 클릭합니다.

단계 **13** **Upload Certificate(**인증서 업로드**)**를 클릭하고 Cisco ISE에서 내보낸 인증서를 업로드합니다.

단계 **14** 인증서가 업로드되면 창에 표시되는 지문 값이 Cisco ISE 인증서의 핑거프린트 값과 일치하는지 확인합니다.

단계 **15** 왼쪽 메뉴 패널에서 **Manifest(**매니페스트**)**를 선택합니다.

단계 **16** 표시되는 콘텐츠에서 **displayName**의 값을 확인합니다. 값은 Cisco ISE 인증서에 나와 있는 공용 이름과 일치해야 합니다.

단계 **17** 왼쪽 메뉴 패널에서 **API Permissions(API** 권한**)**를 선택합니다.

단계 **18** **Add(**추가**)**를 클릭하고 다음 권한을 추가합니다.

API / Permissions name	Type	Description	Admin consent req...	Status
∨ Intune (1)				
get_device_compliance	Application	Get device state and compliance information from Micr...	Yes	Granted
∨ Microsoft Graph (6)				
DeviceManagementConfigurat	Delegated	Read Microsoft Intune Device Configuration and Policies	Yes	Granted
DeviceManagementServiceCo	Delegated	Read Microsoft Intune configuration	Yes	Granted
Directory.Read.All	Delegated	Read directory data	Yes	Granted
Directory.Read.All	Application	Read directory data	Yes	Granted
openid	Delegated	Sign users in	-	Granted
User.Read	Delegated	Sign in and read user profile	-	Granted

단계 **19** 애플리케이션의 **Overview(**개요**)** 창에서 다음 세부정보를 수집합니다.

- 애플리케이션**(**클라이언트**) ID**
- 디렉토리**(**테넌트**) ID**

단계 **20** **Overview(**개요**)** 창에서 **Endpoints(**엔드포인트**)**를 클릭하고 **Oauth 2.0 Token Endpoint (V2)(Oauth 2.0** 토큰 엔드포인트**(V2))** 필드의 값을 복사합니다.

단계 **21** PEM(체인) 형식으로 https://graph.windows.net 및 https://fef.msuc05.manage.microsoft.com/에서 인증서를 다운로드합니다. 다음 인증서를 다운로드해야 합니다.

- Microsoft IT TLS CA 1

- Baltimore CyberTrust Root
- DigiCert SHA2 Secure Server CA
- DigiCert Global Root CA

단계 **22** Cisco ISE 관리 포털에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Certificates(**인증서**)** > **Trusted Certificates(**신뢰할 수 있는 인증서**)**를 선택합니다.

단계 **23** 다운로드한 4개의 인증서 각각에 대해 다음 단계를 수행합니다.

1. **Import(**가져오기**)**를 클릭합니다.
2. **Choose File(**파일 선택**)**을 클릭하고 시스템에서 다운로드한 인증서를 선택합니다.
3. 인프라 및 Cisco Services에서 인증서를 신뢰할 수 있도록 허용합니다. **Usage(**사용**)** 영역에서 **Trust for authentication within ISE(ISE** 내의 인증 신뢰**)** 및 **Trust for authentication of Cisco Services(Cisco Services**의 인증 신뢰**)** 확인란을 선택합니다.
4. **Save(**저장**)**를 클릭합니다.

단계 **24** 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Network Resources(**네트워크 리소스**)** > **External MDM(**외부 **MDM)**을 선택합니다.

단계 **25** **Add(**추가**)**를 클릭합니다.

단계 **26** **Name(**이름**)** 필드에 값을 입력합니다.

단계 **27** **Authentication Type(**인증 유형**)** 드롭다운 목록에서 **OAuth – Client Credentials(OAuth -** 클라이언트 자격 증명**)**를 선택합니다.

단계 **28** 다음 필드에는 Microsoft Azure Active Directory의 Microsoft Intune 애플리케이션의 정보가 필요합니다.

1. **Auto Discovery URL(**자동 검색 **URL)** 필드에 “https://graph.windows.net/<디렉토리*(*테넌트*) ID*>”를 입력합니다.
2. **Client ID(**클라이언트 **ID)** 필드에 Microsoft Intune 애플리케이션의 애플리케이션**(**클라이언트**) ID** 값을 입력합니다.
3. **Token Issuing URL(**토큰 발급 **URL)** 필드에 **Oauth 2.0** 토큰 엔드포인트**(V2)** 값을 입력합니다.

단계 **29** **Polling Interval(**폴링 간격**)** 및 **Time Interval For Compliance Device ReAuth Query(**규정 준수 디바이스 재인증 쿼리 시간 간격**)** 필드에 원하는 값을 입력합니다.

단계 **30** **Test Connection(**연결 테스트**)**을 클릭하여 Cisco ISE에서 Microsoft 서버에 연결할 수 있는지 확인합니다.

단계 **31** 연결 테스트에 성공하면 **Status(**상태**)** 드롭다운 목록에서 **Enabled(**활성화됨**)**를 선택합니다.

단계 **32** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

Cisco ISE 관리 포털에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Network Resources(**네트워크 리소스**)** > **External MDM(**외부 **MDM)**을 클릭합니다. 추가된 Microsoft Intune 서버가 표시된 **MDM Server(MDM** 서버**)** 목록에 나타나야 합니다.

Microsoft System Center Configuration Manager용 정책 집합 예

Microsoft SCCM을 지원하기 위해 다음과 같은 새로운 사전 항목을 정책에서 사용할 수 있습니다.

- **MDM.DaysSinceLastCheckin**: 사용자가 마지막으로 Microsoft SCCM에 디바이스를 체크인하거나 동기화한 이후 경과된 기간(일)입니다. 유효한 값 범위는 1일~365일입니다.
- **MDM.UserNotified**: 유효한 값은 **Y** 또는 **N**입니다. 이 값은 사용자에게 디바이스가 등록되지 않았다는 알림을 받았는지를 나타냅니다. 그런 다음 사용자는 네트워크에 대한 제한된 액세스를 허용한 뒤 등록 포털로 리디렉션하거나 네트워크에 대한 액세스를 거부할 수 있습니다.
- **MDM.ServerType**: 유효한 값은 MDM 서버용 **MDM** 및 데스크톱 디바이스 관리용 **DM**입니다.

Microsoft SCCM을 지원하는 정책 집합의 예는 다음과 같습니다.

정책 이름	**If**	**Then**
SCCM_Comp	Wireless_802.1X AND MDM:MDMServerName EQUALS SccmServer1 AND MDM:DeviceRegisterStatus EQUALS Registered	PermitAccess
SCCM_NonComp_Notify	Wireless_802.1X AND MDM:MDMServerName EQUALS SccmServer1 AND MDM:DeviceCompliantStatus EQUALS NonCompliant AND MDM:UserNotified EQUALS 28	PermitAccess
SCCM_NonComp_Days	Wireless_802.1X AND MDM:MDMServerName EQUALS SccmServer1 AND MDM:MDMDeviceCompliantStatus EQUALS Registered AND MDM:DaysSinceLastCheckin EQUALS 28	SCCMRedirect

정책 이름	If	Then
SCCM_NonComp	Wireless_802.1X AND MDM:MDMServerName EQUALS SccmServer1 AND MDM:DeviceCompliantStatus EQUALS NonCompliant AND MDM:DeviceRegisterStatus EQUALS Registered	SCCMRedirect
SCCM_UnReg_Notify	Wireless_802.1X AND MDM:DeviceRegisterStatus EQUALS Registered AND MDM:UserNotified EQUALS Yes	PermitAccess

Cisco ISE에 Microsoft System Center Configuration Manager 서버 구성

Cisco ISE는 WMI(Windows Management Instrumentation)를 사용하여 Microsoft SCCM 서버와 통신합니다. Microsoft SCCM을 실행 중인 Windows 서버에서 WMI를 구성합니다.

참고 Cisco ISE 통합에 사용하는 사용자 계정은 다음 중 하나여야 합니다.

- SMS 관리자 사용자 그룹의 멤버여야 합니다.
- WMI 네임스페이스에서 SMS 개체와 동일한 권한을 갖습니다.

  `root\sms\site_<sitecode>`

  여기서 *sitecode*는 Microsoft SCCM 사이트입니다.

Microsoft Active Directory 사용자가 도메인 관리자 그룹에 있을 때의 권한 설정

Windows Server 2008 R2, Windows Server 2012 및 Windows Server 2012 R2의 경우 도메인 관리자 그룹에는 기본적으로 Windows 운영체제의 특정 레지스트리 키에 대한 모든 제어 권한이 없습니다. Microsoft Active Directory 관리자는 Microsoft Active Directory 사용자에게 다음 레지스트리 키에 대한 모든 제어 권한을 부여해야 합니다.

- **HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}**
- **HKLM\Software\Classes\Wow6432Node\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}**

다음 Microsoft Active Directory 버전의 경우에는 레지스트리를 변경할 필요가 없습니다.

- Windows 2003
- Windows 2003R2

- Windows 2008

모든 제어 권한을 부여하려면 Microsoft Active Directory 관리자가 먼저 다음과 같이 키 소유권을 얻어야 합니다.

단계 **1** 키 아이콘을 마우스 오른쪽 버튼으로 클릭하고 **Owner(**소유자**)** 탭을 선택합니다.

단계 **2** **Permissions(**권한**)**를 클릭합니다.

단계 **3** **Advanced(**고급**)**를 클릭합니다.

도메인 관리자 그룹에 속하지 않은 **Microsoft Active Directory** 사용자에 대한 권한

Windows 2012 R2의 경우 Microsoft AD 사용자에게 다음 레지스트리 키에 대한 모든 제어 권한을 부여합니다.

- `HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}`
- `HKLM\Software\Classes\Wow6432Node\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}`

Windows PowerShell에서 다음 명령을 사용하여 레지스트리 키에 대한 전체 권한이 부여되었는지 확인합니다.

- ```
  get-acl -path
  "Microsoft.PowerShell.Core\Registry::HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}"
  | format-list
  ```
- ```
  get-acl -path
  "hklm:\Software\Classes\Wow6432Node\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}" |
  format-list
  ```

Microsoft AD 사용자가 도메인 관리자 그룹에는 없지만 도메인 사용자 그룹에는 있으면 다음 권한이 필요합니다.

- Cisco ISE가 도메인 컨트롤러에 연결할 수 있도록 레지스트리 키 추가
- 도메인 컨트롤러에서 DCOM을 사용하기 위한 권한
- WMI 루트/CIMv2 이름 공간에 대한 액세스 권한 설정

이러한 권한은 다음 Microsoft AD 버전에만 필요합니다.

- Windows 2003
- Windows 2003R2
- Windows 2008
- Windows 2008 R2
- Windows 2012

- Windows 2012 R2
- Windows 2016

Cisco ISE가 도메인 컨트롤러에 연결할 수 있도록 레지스트리 키 추가

Cisco ISE가 도메인 사용자로 연결하여 로그인 인증 이벤트를 검색할 수 있게 하려면 도메인 컨트롤러에 일부 레지스트리 키를 수동으로 추가해야 합니다. 도메인 컨트롤러 또는 도메인의 머신에서 에이전트는 필요하지 않습니다.

다음 레지스트리 스크립트에는 추가할 키가 나와 있습니다. 이 스크립트를 복사하여 텍스트 파일에 붙여 넣고 파일을 .reg 확장자로 저장한 다음 파일을 더블 클릭하여 레지스트리를 변경합니다. 레지스트리 키를 추가하려면 사용자가 루트 키의 소유자여야 합니다.

```
Windows Registry Editor Version 5.00

[HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}]
"AppID"="{76A64158-CB41-11D1-8B02-00600806D9B6}"

[HKEY_CLASSES_ROOT\AppID\{76A64158-CB41-11D1-8B02-00600806D9B6}]
"DllSurrogate"="  "

[HKEY_CLASSES_ROOT\Wow6432Node\AppID\{76A64158-CB41-11D1-8B02-00600806D9B6}]
"DllSurrogate"="  "
```

DllSurrogate 키의 값에는 공백이 두 개 포함되어야 합니다. 레지스트리를 수동으로 업데이트하는 경우 두 개의 공백만 포함하고 따옴표는 포함하지 않아야 합니다. 레지스트리를 수동으로 업데이트하는 동안 AppID, DllSurrogate 및 해당 값에 따옴표가 포함되지 않았는지 확인하십시오.

파일 맨 끝의 빈 줄을 포함하여 위 스크립트에 나와 있는 빈 줄은 그대로 유지합니다.

Windows 명령 프롬프트에서 다음 명령을 사용하여 레지스트리 키가 생성되었고 올바른 값을 가지고 있는지 확인합니다.

- `reg query "HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}" /f "{76A64158-CB41-11D1-8B02-00600806D9B6}" /e`
- `reg query HKEY_CLASSES_ROOT\AppID\{76A64158-CB41-11D1-8B02-00600806D9B6} /f "  " /e`
- `reg query HKEY_CLASSES_ROOT\Wow6432Node\AppID\{76A64158-CB41-11D1-8B02-00600806D9B6} /f "  " /e`

도메인 컨트롤러에서 **DCOM**을 사용하기 위한 권한

Cisco ISE 패시브 ID 서비스에 사용되는 Microsoft Active Directory 사용자는 도메인 컨트롤러 서버에서 DCOM을 사용할 권한이 있어야 합니다. **dcomcnfg** 명령줄 도구를 사용하여 권한을 구성하십시오.

단계 **1** 명령줄에서 **dcomcnfg** 도구를 실행합니다.

단계 **2** **Component Services(**구성 요소 서비스**)**를 펼칩니다.

단계 **3** **Computers(**컴퓨터**)** > **My Computer(**내 컴퓨터**)**를 펼칩니다.

단계 **4** 메뉴 모음에서 **Action(**작업**)**을 선택하고 **Properties(**속성**)**를 클릭한 후 **COM Security(COM** 보안**)**를 클릭합니다.

단계 **5** Cisco ISE가 액세스 및 실행에 모두 사용할 계정에 Allow(허용) 권한이 있는지 확인합니다. 해당 Microsoft Active Directory 사용자를 4개 옵션(**Access Permissions(**액세스 권한**)** 및 **Launch and Activation Permissions(**실행 및 활성화 권한**)** 모두에 대한 **Edit Limits(**제한 편집**)**와 **Edit Default(**기본값 편집**))**에 모두 추가해야 합니다.

단계 **6** **Access Permissions(**액세스 권한**)** 및 **Launch and Activation Permissions(**실행 및 활성화 권한**)** 둘 다에 대해 로컬 액세스 및 Remote Access를 모두 허용합니다.

그림 ***5:*** 액세스 권한에 대한 로컬 및 ***Remote Access***

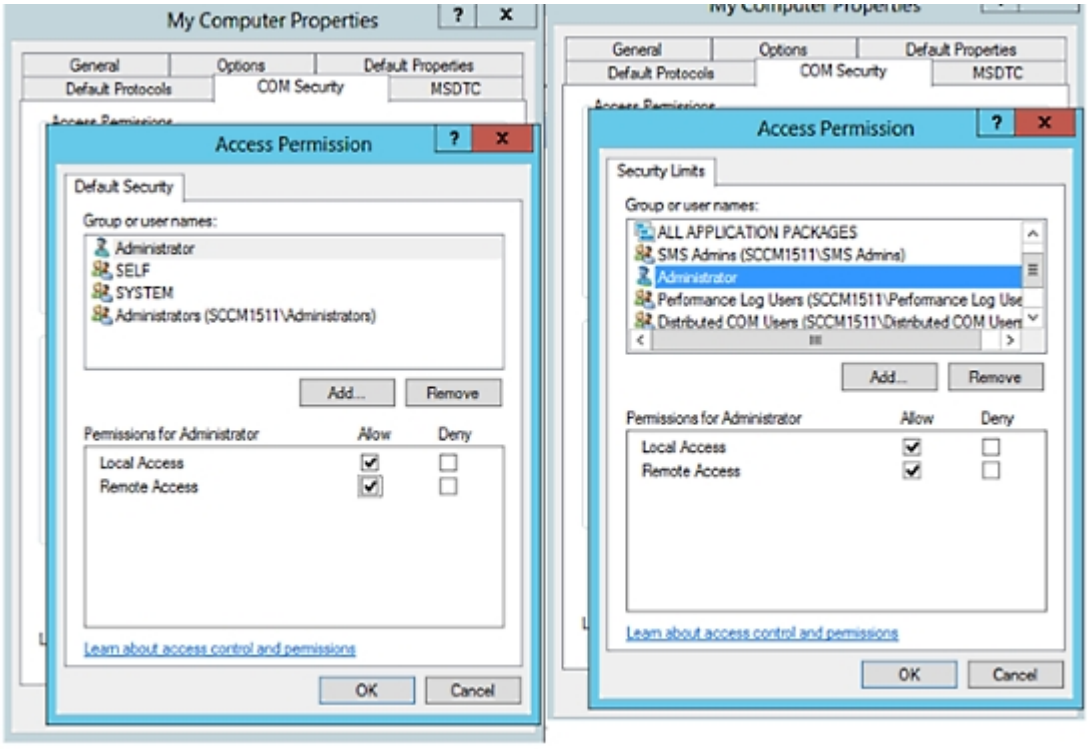
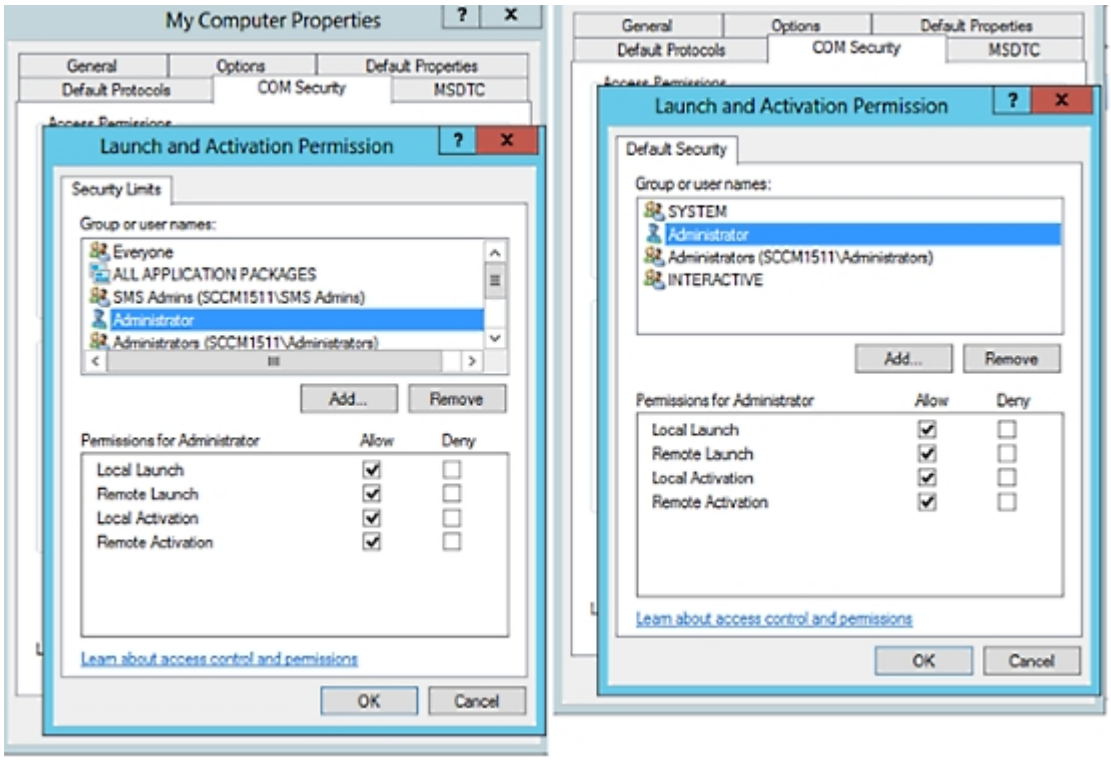


그림 *6:* 실행 및 활성화 권한에 대한 로컬 및 ***Remote Access***



WMI 루트/CIMv2 이름 공간에 대한 액세스 권한 설정

기본적으로 Microsoft Active Directory 사용자에게는 방법 실행 및 원격 활성화에 대한 권한이 없습니다. wmimgmt.msc MMC 콘솔을 사용하여 액세스 권한을 부여할 수 있습니다.

단계 **1** **Start(**시작**)** > **Run(**실행**)**을 선택하고 `wmimgmt.msc`를 입력합니다.

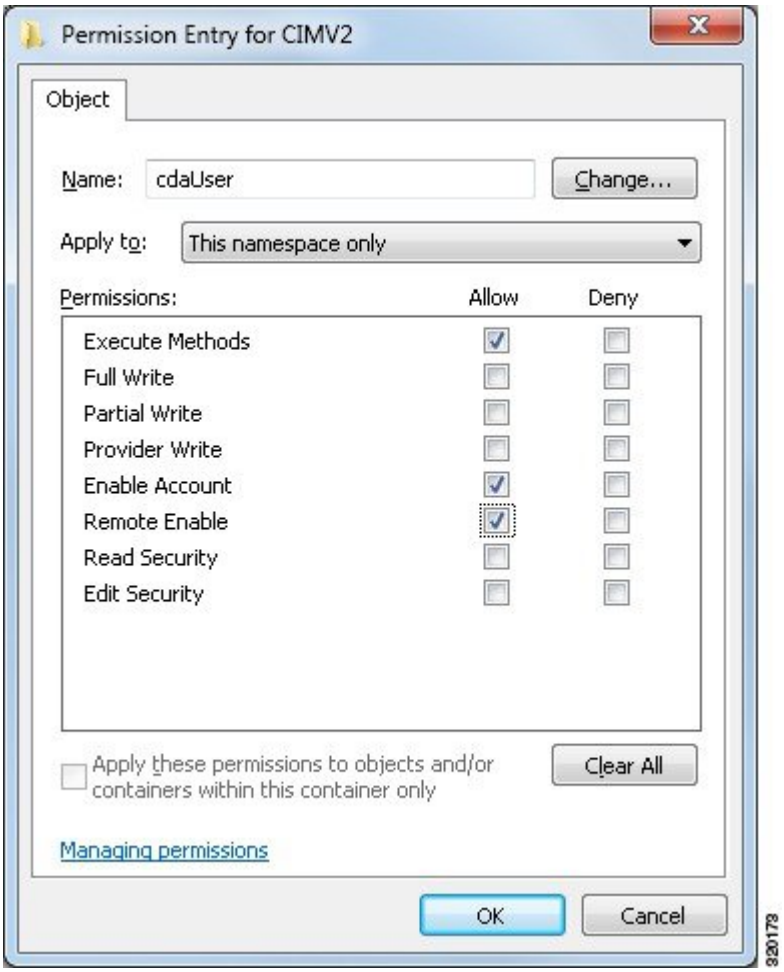
단계 **2** **WMI Control(WMI** 컨트롤**)**을 마우스 오른쪽 버튼으로 클릭하고 **Properties(**속성**)**를 클릭합니다.

단계 **3** **Security(**보안**)** 탭에서 **Root(**루트**)**를 펼치고 **CIMV2**를 선택합니다.

단계 **4** **Security(**보안**)**를 클릭합니다.

단계 **5** Active Directory 사용자를 추가하고 아래 이미지에 나와 있는 대로 필요한 권한을 구성합니다.

그림 *7: WMI Root\CIMv2* 이름 공간에 필요한 권한



WMI 액세스를 위한 방화벽 포트 열기

Microsoft Active Directory 도메인 컨트롤러의 방화벽 소프트웨어가 WMI에 대한 액세스를 차단할 수 있습니다. 방화벽을 끄거나, 특정 IP(Cisco ISE IP 주소)에서의 다음 포트에 대한 액세스를 허용할 수 있습니다.

- TCP 135: 일반 RPC 포트입니다. 비동기 RPC 호출을 수행하는 경우, 이 포트에서 수신 대기하는 서비스는 이 요청을 서비스하는 구성 요소에서 사용 중인 포트를 클라이언트에 알립니다.
- UDP 138: NetBIOS 데이터그램 서비스
- TCP 139: NetBIOS 세션 서비스
- TCP 445: SMB

참고 Cisco ISE는 SMB 2.0을 지원합니다.

더 많은 포트가 동적으로 할당됩니다. 또는 수동으로 구성할 수 있습니다. 대상으로 *%SystemRoot%\System32\dllhost.exe*를 추가하는 것을 권장합니다. 이 프로그램은 포트를 동적으로 관리합니다.

모든 방화벽 규칙을 특정 IP(Cisco ISE IP)에 할당할 수 있습니다.

데스크톱 디바이스 관리자 서버에서 엔드포인트 규정 준수에 대한 구성 베이스라인 정책 선택

Cisco ISE에 추가된 데스크톱 디바이스 관리자 서버(예 : Microsoft SCCM 서버)에서 사용 가능한 베이스라인 정책을 확인하고 네트워크 액세스에 대한 엔드포인트 규정 준수를 확인하는 데 사용할 특정 베이스라인 정책을 선택할 수 있습니다. 데스크톱 디바이스 관리자 서버에서 활성화되고 구축된 구성 베이스라인 정책은 Cisco ISE 관리 포털에서 확인할 수 있습니다.

참고 데스크톱 디바이스 관리 서버에서 사용자 권한을 검토하여 베이스라인 정책 및 규정 준수 정보를 Cisco ISE로 전송하는 데 필요한 보안 권한이 있는지 확인하십시오. 관리자는 데스크톱 디바이스 관리자의 **Security(**보안**) > Administrator Users(**관리자**)** 폴더에 추가해야 합니다.

Cisco ISE GUI에서 데스크톱 디바이스 관리자 서버의 베이스라인 정책을 보려면 **Menu(**메뉴**)** 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Network Resources(**네트워크 리소스**)** > **External MDM(**외부 **MDM)** > **MDM Servers(MDM** 서버**)**를 선택합니다.

Cisco ISE에 새 데스크톱 디바이스 관리자 서버 추가 및 구성 베이스라인 정책 선택

1. **MDM Servers(MDM** 서버**)** 창에서 **Add(**추가**)**를 클릭합니다.
2. **Server Type(**서버 유형**)** 드롭다운 목록에서 **Desktop Device Manager(**데스크톱 디바이스 관리자**)**를 선택합니다.
3. 다음 필드의 필수 세부 사항을 입력합니다.
   - **Host Name / IP Address(**호스트 이름**/IP** 주소**)**: Microsoft SCCM 서버의 호스트 이름 또는 IP 주소를 입력합니다.
   - **Instance Name(**인스턴스 이름**)**: Microsoft SCCM 서버에 인스턴스가 여러 개 있는 경우 연결하려는 인스턴스를 입력합니다.
   - **Username(**사용자 이름**)**: Microsoft SCCM 서버에 연결하는 데 사용해야 하는 사용자 이름을 입력합니다.
   - **Password(**비밀번호**)**: Microsoft SCCM 서버에 연결하는 데 사용해야 하는 비밀번호를 입력합니다.

- **Time Interval For Compliance Device ReAuth Query(**규정 준수 디바이스 재인증 쿼리 시간 간격**)**: 엔드포인트가 인증되거나 재인증되는 경우 Cisco ISE는 캐시를 사용하여 해당 엔드포인트에 대한 MDM 변수를 가져옵니다. 캐시된 값의 기간이 이 필드에 구성된 값보다 높은 경우 Cisco ISE는 새 디바이스 쿼리를 MDM 서버로 보내 새 값을 가져옵니다. 규정 준수 상태가 변경된 경우 Cisco ISE는 적절한 CoA를 트리거합니다.

  유효 범위는 1분~1440분입니다. 기본값은 1분입니다.

4. **Status(**상태**)** 드롭다운 목록에서 **Enabled(**활성화됨**)**를 선택합니다.

서버가 Cisco ISE에 연결되어 있는지 확인하려면 **Test Connection(**연결 테스트**)** 버튼을 클릭합니다. 이 서버에서 사용 가능한 구성 베이스라인 정책을 보려면 **Save & Continue(**저장 후 계속**)**를 클릭합니다. 베이스라인 정책의 이름 및 ID 목록이 포함된 새 창이 표시됩니다.

기존 데스크톱 디바이스 관리자 서버에서 구성 베이스라인 정책 선택

MDM Servers(MDM 서버**)** 창에서 원하는 서버의 확인란을 선택하고 **Edit(**편집**)**를 클릭합니다. 이 서버에서 사용 가능한 베이스라인 정책 목록을 보려면 **Configuration Baselines(**구성 베이스라인**)** 탭을 클릭합니다.

기본적으로 모든 베이스라인 정책이 선택됩니다. **Name(**이름**)** 옆의 확인란을 선택 취소하여 모든 베이스라인 정책을 선택 취소합니다. 해당 이름 옆의 확인란을 선택하여 필요한 베이스라인 정책을 선택합니다. **Save(**저장**)**를 클릭합니다.

엔드포인트 규정 준수는 선택한 구성 베이스라인 정책에 따라 확인됩니다.

데스크톱 디바이스 관리자 서버의 구성 베이스라인 정책에 변경 사항이 있는 경우 **Configuration Baselines(**구성 베이스라인**)** 탭에서 **Update Now(**지금 업데이트**)** 버튼을 클릭하여 Cisco ISE에서 업데이트할 변경 사항을 확인합니다.

Windows 엔드포인트에 대한 디바이스 식별자 구성

데스크톱 디바이스 관리자 서버는 특정 속성을 식별자로 사용하여 네트워크에 연결하는 엔드포인트를 확인합니다. 엔드포인트 MAC 주소가 가장 많이 사용되는 식별자입니다. 그러나 동글, 도킹 스테이션 또는 MAC 주소 임의 지정 기술을 사용하는 경우 MAC 주소가 그다지 신뢰할 수 있는 식별자가 아닙니다.

이제 호스트 이름을 식별자로 사용하도록 선택할 수 있습니다. 호스트 이름은 인증서에서 사용 가능한 CN(Common Name) 또는 SAN-DNS 속성에서 파생됩니다. 엔드포인트의 인증서 기반 인증은 호스트 이름을 사용하여 베이스라인 정책 규정 준수를 확인하는 데 필수입니다.

데스크톱 디바이스 관리자 서버의 디바이스 식별자를 구성하려면 해당 **Server Configuration(**서버 구성**)** 탭으로 이동합니다. 메인 메뉴에서 **Administration(**관리**)** > **Network Resources(**네트워크 리소스**)** > **External MDM(**외부 **MDM)** > **MDM Servers(MDM** 서버**)** > **Edit(**편집**)**를 선택합니다.

Device Identifier Configurations(디바이스 식별자 구성**)** 섹션에서는 다음 식별자가 나열된 순서대로 기본적으로 활성화되어 있습니다.

1. 레거시 **MAC** 주소
2. 인증서 **- CN,** 호스트 이름

3. 인증서 - **SAN-DNS,** 호스트 이름

식별자를 선택 취소하려면 식별자에 대한 확인란을 선택 취소합니다. 속성을 끌어 서버에서 확인에 사용하는 순서를 재배열할 수 있습니다.

디바이스 식별자의 구성 확인

호스트 이름을 확인에 사용하는 경우 Cisco ISE에서 엔드포인트에 GUID가 할당됩니다. **Live Logs(**라이브 로그**)** 창(Cisco ISE GUI에서 **Menu(**메뉴**)** 아이콘(☰)을 클릭하고**Operations(**운영**)** > **RADIUS** > **Live Logs(**라이브 로그**)** 선택)에서 GUID 항목의 세부정보를 확인합니다.

미등록 디바이스 리디렉션을 위한 권한 부여 프로파일 구성

각 외부 MDM 서버에 대해 미등록 디바이스를 리디렉션하도록 Cisco ISE에서 권한 부여 프로파일을 구성해야 합니다.

시작하기 전에

- Cisco ISE에서 MDM 서버 정의를 생성했는지 확인합니다. Cisco ISE를 MDM 서버와 정상적으로 통합해야 MDM 사전이 채워지며 MDM 사전 속성을 사용하여 권한 부여 정책을 생성할 수 있습니다.
- 미등록 디바이스 리디렉션을 위해 Wireless LAN Controller에서 ACL을 구성합니다.
- 인터넷 연결에 프록시를 사용하며 MDM 서버가 내부 네트워크에 속해 있는 경우에는 프록시-우회 목록에 MDM 서버의 이름이나 해당 IP 주소를 포함해야 합니다. 이 작업을 수행하려면 Cisco ISE GUI에서 **Menu(**메뉴**)** 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Settings(**설정**)** > **Proxy(**프록시**)**를 선택합니다.

단계 **1** Cisco ISE GUI에서 **Menu(**메뉴**)** 아이콘(☰)을 클릭하고 **Policy(**정책**)** > **Policy Elements(**정책 요소**)** > **Results(**결과**)** > **Authorization(**권한 부여**)** > **Authorization Profiles(**권한 부여 프로파일**)** > **Add(**추가**)**를 선택합니다를 선택합니다.

단계 **2** 규정을 준수하지 않거나 등록되지 않은 미등록 디바이스 리디렉션을 위한 권한 부여 프로파일을 생성합니다.

단계 **3** MDM 서버 이름과 일치하는 권한 부여 프로파일의 이름을 **Name(**이름**)** 필드에 입력합니다.

단계 **4** **Access Type(**액세스 유형**)** 드롭다운 목록에서 **ACCESS_ACCEPT**를 선택합니다.

단계 **5** **Common Tasks(**일반 작업**)** 섹션에서 **Web Redirection(**웹 리디렉션**)** 확인란을 선택하고 드롭다운 목록에서 **MDM Redirect(MDM** 리디렉션**)**를 선택합니다.

단계 **6** **ACL** 드롭다운 목록에서 무선 LAN 컨트롤러에 구성한 ACL의 이름을 선택합니다.

단계 **7** **Value(**값**)** 드롭다운 목록에서 MDM 포털을 선택합니다.

단계 **8** **MDM Server(MDM** 서버**)** 드롭다운 목록에서 사용할 MDM 서버를 선택합니다.

단계 **9** **Submit(**제출**)**을 클릭합니다.

다음에 수행할 작업

모바일 디바이스 관리 활용 사례용으로 권한 부여 정책 규칙 구성.

모바일 디바이스 관리 활용 사례용으로 권한 부여 정책 규칙 구성

MDM 컨피그레이션을 완료하려면 Cisco ISE에서 권한 부여 정책 규칙을 구성해야 합니다.

시작하기 전에

- Cisco ISE 인증서 저장소에 MDM 서버 인증서를 추가합니다.
- Cisco ISE에서 MDM 서버 정의를 생성했는지 확인합니다. Cisco ISE를 MDM 서버와 정상적으로 통합해야 MDM 사전이 채워지며 MDM 사전 속성을 사용하여 권한 부여 정책을 생성할 수 있습니다.
- 미등록 또는 규정 미준수 디바이스 리디렉션을 위해 Wireless LAN Controller에서 ACL을 구성합니다.

단계 **1** Cisco ISE GUI에서 **Menu(**메뉴**)** 아이콘(☰)을 클릭하고 **Policy(**정책**)** > **Policy Sets(**정책 집합**)**을 선택한 다음 정책 집합을 확장하여 권한 부여 정책 규칙을 확인합니다.

단계 **2** 다음 규칙을 추가합니다.

- **MDM_Un_Registered_Non_Compliant**: MDM 서버에 아직 등록되지 않았거나 MDM 정책을 준수하지 않는 디바이스용입니다. 요청이 이 규칙과 일치하면 디바이스를 MDM 서버에 등록하는 방법에 대한 정보가 포함된 Cisco ISE MDM 창이 사용자에게 표시됩니다.

  참고 이 정책에서 **MDM.MDMServerName** 조건을 사용하지 마십시오. 이 조건을 사용하는 경우 엔드포인트가 MDM 서버에 등록된 경우에만 엔드포인트가 정책과 일치합니다.

- **PERMIT**: Cisco ISE와 MDM에 등록되어 있으며 Cisco ISE/MDM 정책을 준수하는 디바이스의 경우 Cisco ISE에 구성된 액세스 제어 정책에 따라 네트워크 액세스 권한이 부여됩니다.

단계 **3** **Save(**저장**)**를 클릭합니다.

모바일 디바이스 관리 상호운용성을 위해 무선 **LAN** 컨트롤러에서 **ACL** 구성

미등록 디바이스 및 인증서 프로비저닝을 리디렉션하려면 권한 부여 정책에 사용할 ACL을 무선 컨트롤러에서 구성해야 합니다. ACL의 순서는 다음과 같이 지정해야 합니다.

단계 **1** 서버에서 클라이언트로의 모든 아웃바운드 트래픽을 허용합니다.

단계 **2** (선택 사항) 문제 해결용으로 클라이언트에서 서버로의 ICMP 클라이언트 인바운드 트래픽을 허용합니다.

단계 **3** 미등록/규정 미준수 디바이스에 대해 MDM 에이전트를 다운로드하고 규정 준수 확인을 진행할 수 있도록 MDM 서버 액세스를 허용합니다.

단계 **4** 웹 포털과 supplicant 및 인증서 프로비저닝 플로우에 대해 클라이언트->서버->Cisco ISE로의 모든 인바운드 트래픽을 허용합니다.

단계 **5** 이름 확인용으로 클라이언트에서 서버로의 인바운드 DNS 트래픽을 허용합니다.

단계 **6** IP 주소용으로 클라이언트에서 서버로의 인바운드 DHCP 트래픽을 허용합니다.

단계 **7** 회사 정책에 따른 Cisco ISE로의 리디렉션용으로 클라이언트->서버->회사 리소스로의 모든 인바운드 트래픽을 거부합니다.

단계 **8** (선택 사항) 나머지 트래픽을 허용합니다.

예

다음 예제에서는 미등록 디바이스를 BYOD 흐름으로 리디렉션하기 위한 ACL을 보여 줍니다. 이 예제에서 Cisco ISE IP 주소는 10.35.50.165, 내부 회사 네트워크 IP 주소는 192.168.0.0 및 172.16.0.0(리디렉션용), MDM 서버 서브넷은 204.8.168.0입니다.

그림 ***8:*** 미등록 디바이스 리디렉션용 ***ACL***

General

Access List Name NSP-ACL

Deny Counters 0

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits
1	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Outbound	150720
2	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	ICMP	Any	Any	Any	Inbound	7227
3	Permit	0.0.0.0 / 0.0.0.0	204.8.168.0 / 255.255.255.0	Any	Any	Any	Any	Any	17626
4	Permit	0.0.0.0 / 0.0.0.0	10.35.50.165 / 255.255.255.255	Any	Any	Any	Any	Inbound	7505
5	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	Any	DNS	Any	Inbound	2864
6	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	Any	DHCP Server	Any	Inbound	0
7	Deny	0.0.0.0 / 0.0.0.0	192.168.0.0 / 255.255.0.0	Any	Any	Any	Any	Inbound	0
8	Deny	0.0.0.0 / 0.0.0.0	172.16.0.0 / 255.240.0.0	Any	Any	Any	Any	Inbound	4
9	Deny	0.0.0.0 / 0.0.0.0	10.0.0.0 / 255.0.0.0	Any	Any	Any	Any	Inbound	457
10	Deny	0.0.0.0 / 0.0.0.0	173.194.0.0 / 255.255.0.0	Any	Any	Any	Any	Inbound	1256
11	Deny	0.0.0.0 / 0.0.0.0	171.68.0.0 / 255.252.0.0	Any	Any	Any	Any	Inbound	11310
12	Deny	0.0.0.0 / 0.0.0.0	171.71.181.0 / 255.255.255.0	Any	Any	Any	Any	Any	0
13	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Any	71819

디바이스 초기화 또는 잠금

Cisco ISE는 분실한 디바이스를 초기화하거나 해당 디바이스에 대해 PIN 잠금을 켤 수 있습니다. **Endpoints(**엔드포인트**)** 창에서 이를 구성할 수 있습니다.

단계 **1** Cisco ISE GUI에서 **Menu(**메뉴**)** 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Network Access(**네트워크 액세스**)** > **Identities(ID)** > **Endpoints(**엔드포인트**)**를 선택합니다.

단계 **2** 초기화하거나 잠글 디바이스 옆의 확인란을 선택합니다.

단계 **3** **MDM Actions(MDM** 작업**)** 드롭다운 목록에서 다음 옵션 중 하나를 선택합니다.

- **Full Wipe(**완전 초기화**)**: MDM 벤더에 따라 이 옵션은 회사 앱을 제거하거나 디바이스를 공장 설정으로 재설정합니다.
- **Corporate Wipe(**회사 초기화**)**: 이 옵션은 MDM 서버 정책에서 구성한 애플리케이션을 제거합니다.
- **PIN Lock(PIN** 잠금**)**: 이 옵션은 디바이스를 잠급니다.

단계 **4** **Yes(**예**)**를 클릭하여 디바이스를 초기화하거나 잠급니다.

Mobile Device Manager 보고서 보기

Cisco ISE는 MDM 서버 정의에 대한 모든 추가, 업데이트 및 삭제 사항을 기록합니다. 이러한 이벤트는 선택한 기간에 걸쳐 시스템 관리자의 모든 컨피그레이션 변경 사항을 제공하는 **Change Configuration Audit(**컨피그레이션 변경 감사**)** 보고서에서 볼 수 있습니다.

Cisco ISE GUI에서 **Menu(**메뉴**)** 아이콘(☰)을 클릭하고 **Operations(**운영**)** > **Reports(**보고서**)** > **Reports(**보고서**)** > **Audit(**감사**)** > **Change Configuration Audit(**컨피그레이션 변경 감사**)**를 선택합니다. 검토하려는 MDM 서버에 대한 **Object Type(**개체 유형**)** 및 **Object Name(**개체 이름**)** 열의 항목을 확인하고 해당 **Event(**이벤트**)** 값을 클릭하여 컨피그레이션 이벤트의 세부정보를 확인합니다.

Mobile Device 관리 로그 보기

Debug Wizard(디버그 마법사) 창을 사용하여 모바일 디바이스 관리 로그 메시지를 볼 수 있습니다. Cisco ISE GUI에서 **Menu(**메뉴**)** 아이콘(☰)을 클릭하고 **Operations(**운영**)** > **Troubleshoot(**문제 해결**)** > **Debug Wizard(**디버그 마법사**)** > **Debug Log Configuration(**디버그 로그 구성**)**을 선택합니다. Cisco ISE 노드 옆의 라디오 버튼을 클릭하고 **Edit(**편집**)**를 클릭합니다. 표시되는 새 창에서 구성 요소 이름 **external-mdm** 옆의 라디오 버튼을 클릭하고 **Edit(**편집**)**를 클릭합니다. 이 구성 요소의 기본 로그 레벨은 **INFO**입니다. 해당 **Log Level(**로그 레벨**)** 드롭 다운 목록에서 **DEBUG** 또는 **TRACE**를 선택하고 **Save(**저장**)**를 클릭합니다.