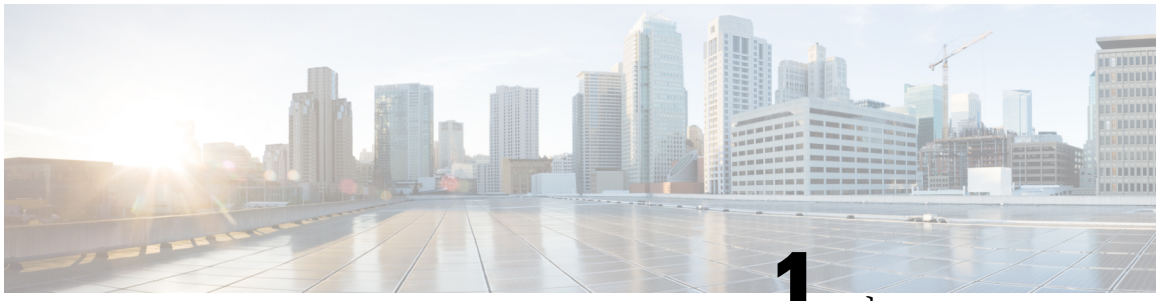
Cisco ISE와 MDM 및 UEM 서버 통합



1 장

Cisco ISE와 UEM 및 MDM 서버 통합

Cisco ISE의 통합 엔드포인트 관리 개요

UEM(Unified Endpoint Management) 또는 MDM(Mobile Device Management) 서버를 사용하여 네트워크에 구축된 엔드포인트를 보호, 모니터링, 관리 및 지원하는 경우 Cisco ISE가 이러한 서버와 상호 운용되도록 구성할 수 있습니다. Cisco ISE 및 엔드포인트 관리 서버를 통합하여 API를 통해 이러한 서버의 디바이스 속성 정보에 액세스합니다. 그런 다음 디바이스 속성을 사용하여 ACL(Access Control List) 및 권한 부여 정책을 생성하여 네트워크 액세스 제어를 활성화할 수 있습니다.

이 문서에서는 엔드포인트 관리 서버를 Cisco ISE와 통합하기 위해 엔드포인트 관리 서버에서 수행해야 하는 구성에 대해 자세히 설명합니다. 이 문서에서는 현재 다음 MDM 또는 UEM 벤더에 필요한 구성을 자세히 설명합니다.

- Cisco0 Meraki Systems Manager
- Ivanti(이전 명칭 MobileIron UEM) 코어 및 클라우드 UEM 서비스
- Microsoft Endpoint Manager Intune

Cisco ISE는 다음 엔드포인트 관리 서버도 지원합니다.

- 42Gears
- Absolute
- Blackberry - BES
- Blackberry - Good Secure EMM

- Citrix XenMobile 10.x(온프레미스)
- Globo
- IBM MaaS360
- JAMF Casper Suite
- Microsoft 엔드포인트 구성 관리자
- Mosyle
- SAP Afaria
- Sophos
- SOTI MobiControl
- Symantec
- Tangoe
- VMware Workspace ONE(이전 AirWatch)

Cisco ISE에 연결하려는 MDM 또는 UEM 서버에서 필요한 구성을 수행한 후에는 서버를 Cisco ISE에 가입시켜야 합니다. 해당 릴리스의 *Cisco ISE 관리자 가이드*에서 "보안 액세스" 장의 "Cisco ISE에서 모바일 디바이스 관리 서버 구성"을 참조하십시오.

GUID용 Cisco ISE MDM API 버전 3

Cisco ISE 릴리스 3.1에는 엔드포인트의 임의 및 변경 MAC 주소를 처리하는 기능이 도입되었습니다. Cisco ISE MDM API 버전 3을 사용하여 연결된 MDM 및 UEM 서버에서 GUID라는 고유한 엔드포인트 식별자를 수신할 수 있습니다. 그런 다음 Cisco ISE는 GUID를 사용하여 MAC 주소 대신 엔드포인트를 식별합니다. 해당 릴리스의 *Cisco ISE 관리자 가이드*의 "보안 액세스" 장에서 "모바일 디바이스 관리 서버를 사용하여 임의 및 변경 MAC 주소 처리"를 참조하십시오.

UEM 또는 MDM 서버에서 GUID를 수신하려면 다음 조건을 충족해야 합니다.

- UEM 또는 MDM 서버는 Cisco ISE MDM API 버전 3을 지원합니다.
- UEM 또는 MDM에서 Cisco ISE 사용을 위한 인증서는 Subject Alternative Name(주체 대체 이름) 필드, Common Name(공용 이름) 필드 또는 둘 다에서 GUID를 Cisco ISE에 푸시하도록 구성됩니다.

다음 UEM 또는 MDM 서버는 현재 Cisco ISE MDM API 버전 3을 지원합니다.

- Cisco0 Meraki Systems Manager
- Ivanti(이전 명칭 MobileIron UEM) 코어 및 클라우드 UEM 서비스
- Microsoft Endpoint Manager Intune

VPN 연결 엔드포인트의 MAC 주소

Cisco ISE는 엔드포인트의 MAC 주소를 사용하여 데이터베이스에 엔드포인트 데이터를 저장 및 관리하고, 상황 가시성 정보를 표시하고, 권한 부여 워크플로를 활성화합니다.

VPN 연결 엔드포인트의 경우, VPN 헤드엔드는 일반적으로 Cisco Secure Client(이전의 Cisco AnyConnect)에서 엔드포인트의 MAC 주소나 UDID(고유 디바이스 식별자) 또는 둘 다를 수신한 다음 RADIUS 통신을 통해 Cisco ISE에 정보를 전송합니다. .

Cisco ISE를 MDM 서버와 통합하는 경우 Cisco ISE는 엔드포인트의 MAC 주소 또는 UDID를 사용하여 엔드포인트의 등록 및 규정 준수 상태와 기타 MDM 속성 값을 MDM 서버에 쿼리합니다.

Cisco ISE가 엔드포인트의 UDID를 사용하여 MDM 서버를 쿼리하는 경우, 일반적으로 MDM 서버의 규정 준수 응답에는 엔드포인트의 MAC 주소가 포함됩니다. Cisco ISE에서는 Cisco Secure Client 또는 MDM 서버에서 엔드포인트의 MAC 주소를 수신하는 것이 중요합니다. Cisco ISE는 MAC 주소를 사용하여 데이터베이스에 엔드포인트 데이터를 저장하고 관리합니다.

Cisco Meraki Systems Manager 구성

Cisco Meraki Systems Manager는 다양한 플랫폼을 지원하여 오늘날 일반적인 다양한 디바이스 에코시스템을 활성화합니다. Systems Manager는 성장하는 조직을 위한 광범위한 확장성과 함께 엔드포인트 관리를 위한 중앙 집중식 클라우드 기반 툴을 제공합니다. Cisco Meraki Systems Manager를 Cisco ISE에서 MDM 서버로 통합하여 Cisco Meraki Systems Manager가 컴플라이언스 확인 및 엔드포인트 정책 관리를 위해 수집하는 엔드포인트 정보를 활용합니다.

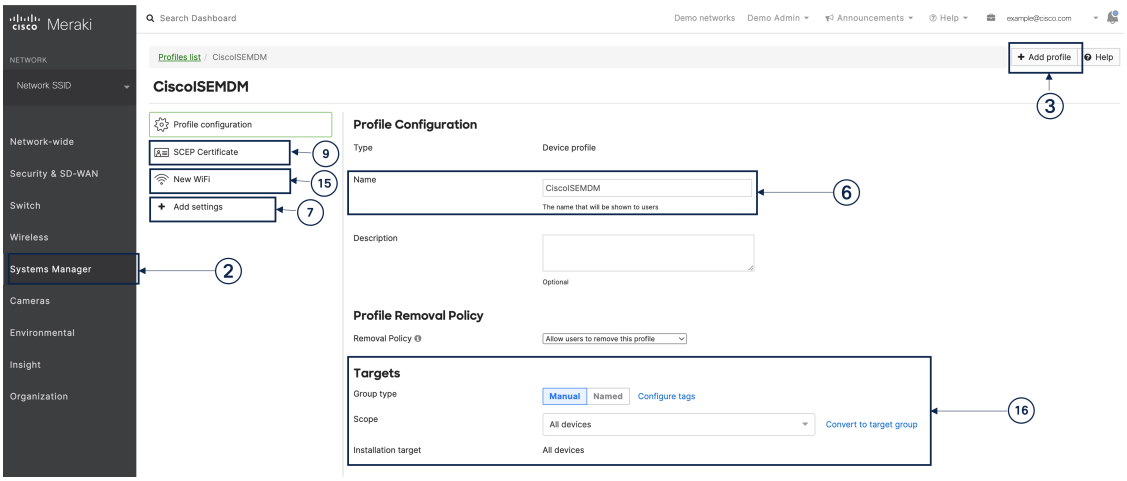
Cisco Meraki Systems Manager에 대한 자세한 내용은 데이터 시트를 참조하십시오.

Cisco Meraki Systems Manager는 이제 MDM API 버전 3을 지원하며 Cisco ISE에 연결된 엔드포인트에 대한 고유한 디바이스 식별자를 제공할 수 있습니다. Cisco ISE에 활성 Cisco Meraki Systems Manager 통합이 이미 있는 경우 Cisco Meraki Systems Manager에서 Cisco ISE 관련 디바이스 프로파일에 대해 8~15단계를 수행합니다.

Cisco Meraki Systems Manager를 MDM/UEM 서버로 구성

이 섹션의 이미지는 이 작업 중에 작업해야 하는 Cisco Meraki Systems Manager GUI 필드를 표시합니다. 이미지의 숫자는 작업의 단계 번호에 해당합니다.

그림 *1: Cisco Merki Systems Manager*를 구성하는 단계



시작하기 전에

Cisco ISE에서 관리자용으로 구성된 시스템 인증서를 생성하고 내보냅니다. 다음 작업의 12단계에서 이 인증서를 사용합니다.

시스템 인증서를 생성하고 내보내는 방법에 대한 지침은 해당 릴리스의 *Cisco ISE* 관리자 가이드에서 "기본 설정" 장의 "시스템 인증서" 항목을 참조하십시오.

단계 **1** Cisco Meraki Systems Manager 포털에 로그인합니다.

단계 **2** 기본 메뉴에서 **Systems Manager(**시스템 관리자**)** > **Manage(**관리**)** > **Settings(**설정**)**로 이동합니다.

단계 **3** **+ Add Profile(**프로파일 추가**)**을 클릭합니다.

단계 **4** 표시되는 Add New Profile(새 프로파일 추가) 대화 상자에서 **Device profile (Default)(**디바이스 프로파일**(**기본값**))** 라디오 버튼을 클릭합니다.

단계 **5** **Continue(**계속**)**를 클릭합니다.

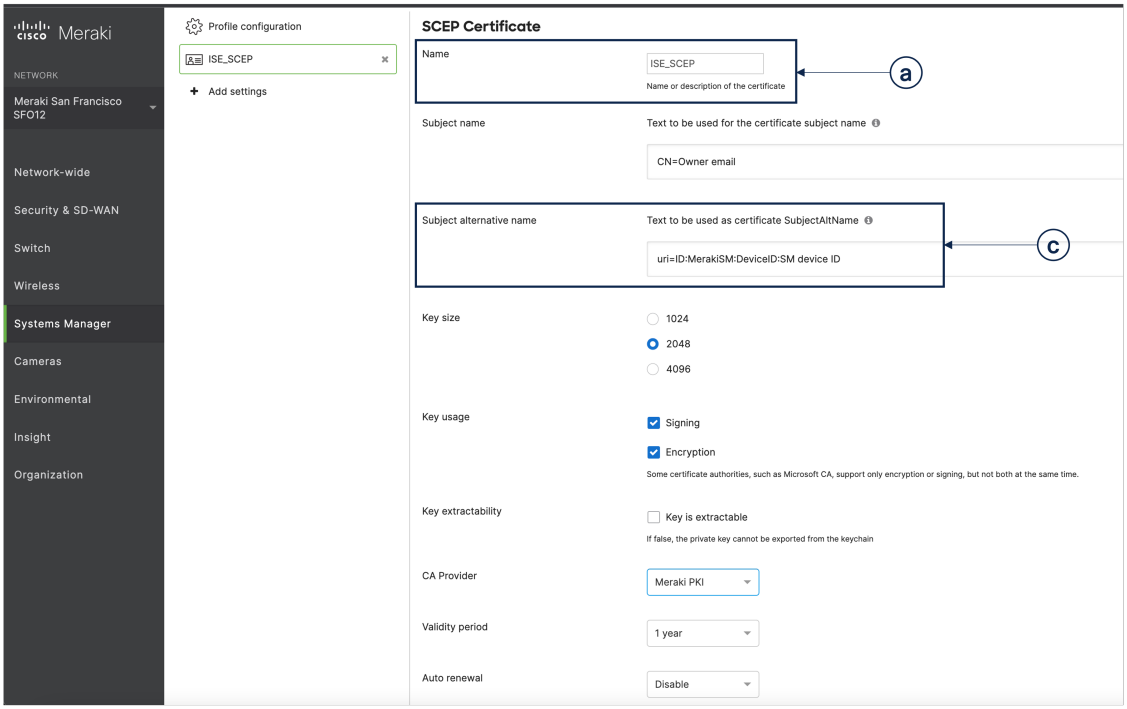
단계 **6** **Name(**이름**)** 및 **Description(**설명**)** 필드에 값을 입력합니다.

단계 **7** **+Add settings(+**설정 추가**)**를 클릭합니다.

단계 **8** 표시되는 **Add New Settings Payload(**새 설정 페이로드 추가**)** 창에서 **SCEP Certificate(SCEP** 인증서**)**를 클릭합니다.

단계 **9** 표시되는 **SCEP Certificate(SCEP** 인증서**)** 창에서 다음 작업을 수행합니다.

그림 *2: Cisco Meraki Systems Manager*의 *SCEP* 인증서 구성 창



a) **Name(**이름**)** 필드에 SCEP 인증서의 이름을 입력합니다. 예: **ISE_SCEP**.
b) **Subject name(**주체 이름**)** 필드에 인증서의 공통 이름 값을 입력합니다.
c) **Subject alternative name(**주체 대체 이름**)** 필드에 **uri=ID:MerakiSM:DeviceID:$SM Device ID**를 입력합니다.

   $를 입력하면 변수의 드롭다운 목록이 표시됩니다. 목록에서 SM Device ID(SM 디바이스 ID)를 선택합니다.

d) **Key Size(**키 크기**)** 영역에서 **2048** 라디오 버튼을 클릭합니다.
e) **Key Usage(**키 사용**)** 영역에서 **Signing(**서명**)** 및 **Encryption(**암호화**)** 확인란을 선택합니다.
f) **CA Provider(CA** 공급자**)** 영역에서 드롭다운 목록에서 CA 공급자를 선택합니다.
g) **Save(**저장**)**를 클릭합니다.

단계 **10** **+Add settings(+**설정 추가**)**를 클릭합니다.

단계 **11** 표시되는 **Add New Settings Payload(**새 설정 페이로드 추가**)** 창에서 **Certificate(**인증서**)**를 클릭합니다.

단계 **12** 표시되는 **Certificate(**인증서**)** 창에서 다음 작업을 수행합니다.

a) **Name(**이름**)** 필드에 인증서의 이름을 입력합니다.
b) **CertStore** 드롭다운 목록에서 **System(**시스템**)**을 선택합니다.
c) **Certificate(**인증서**)** 필드에서 **Choose File(**파일 선택**)**을 클릭하고 이 작업의 사전 요구 사항 단계로 다운로드한 Cisco ISE 시스템 인증서를 업로드합니다.
d) **Save(**저장**)**를 클릭합니다.

단계 **13** **+Add settings(+**설정 추가**)**를 클릭합니다.

단계 **14** 표시되는 **Add New Settings Payload(**새 설정 페이로드 추가**)** 창에서 **WiFi Settings(WiFi** 설정**)**를 클릭합니다.

단계 **15** 표시되는 **WiFi Settings(WiFi** 설정**)** 창에서 다음을 수행합니다.

a) **SSID** 필드에 가입할 Wi-Fi 네트워크의 이름을 입력합니다.
b) **Security(**보안**)** 드롭다운 목록에서 WPA(Wi-Fi Protected Access) 옵션 중 하나를 선택합니다.
c) Security(보안) 드롭다운 목록에서 엔터프라이즈 옵션을 선택하면 표시되는 **Enterprise Settings(**엔터프라이즈 설정**)** 영역에서 다음을 수행합니다.

1. **Protocol(**프로토콜**)** 탭에서 TLS와 같은 인증서 기반 프로토콜의 확인란을 선택합니다.
2. **Authentication(**인증**)** 탭의 **Identity Certificate(ID** 인증서**)** 영역에 있는 드롭다운 목록에서 Cisco ISE 사용 사례(10단계)에 대해 생성한 SCEP 인증서를 선택합니다.
3. **Trust(**신뢰**)** 탭의 **Trusted Certificates(**신뢰할 수 있는 인증서**)** 영역에서 12단계에서 업로드한 Cisco ISE 인증서 옆의 확인란을 선택합니다.
4. **Save(**저장**)**를 클릭합니다.

단계 **16** **Profile Configuration(**프로파일 구성**)** 탭의 **Targets(**대상**)** 영역에서 ISE 사용 사례에 대한 태그를 추가합니다. Meraki Systems Manager에서 태그를 생성하고 관리하는 방법에 대한 자세한 내용은 태그 관리를 참고하십시오. 태그를 적용하면 인증서 및 Wi-Fi 설정이 포함된 ISE 프로파일이 관련 디바이스에 적용됩니다.

단계 **17** **You have unsaved changes(**저장하지 않은 변경 사항이 있습니다**)** 대화 상자에서 **Save(**저장**)**를 클릭합니다.

단계 **18** 왼쪽 메뉴 창에서 **Organization(**조직**) > Configure(**구성**) > MDM**을 선택합니다.

단계 **19** ISE Settings(ISE 설정) 영역에서 다음 작업을 수행합니다.

a) Cisco ISE에 입력해야 하는 사용자 이름 및 암호 세부 정보를 기록해 둡니다.
b) Cisco ISE에서 사용해야 하는 SCEP 인증서를 다운로드하려면 **Download(**다운로드**)** 버튼을 클릭합니다.

다음에 수행할 작업

이제 Cisco Meraki 시스템 관리자를 Cisco ISE에서 MDM 서버로 연결합니다. 이 작업을 수행하는 방법에 대한 자세한 내용은 해당 릴리스의 *Cisco ISE* 관리자 가이드에서 "보안 액세스" 장의 "Cisco ISE에서 모바일 디바이스 관리 서버 구성"을 참조하십시오.

Microsoft Endpoint Manager Intune 구성

다음 단계에는 일반적으로 Microsoft Endpoint Manager Intune에서 수행하는 구성이 나와 있습니다. 조직의 요구에 따라 구현해야 하는 단계를 선택합니다. Cisco ISE 릴리스 3.1을 사용 중이며 Cisco ISE MDM API v3 지원을 활성화하여 Microsoft Intune에서 GUID를 수신하려는 경우, 2단계 및 3단계에 지정된 대로 인증서 프로파일에서 SAN(주체 대체 이름)을 구성합니다. SAN 구성을 사용하면 Cisco ISE가 Intune 서버에서 엔드포인트에 대한 고유한 GUID를 수신하여 임의 및 변경 MAC 주소에서 발생하는 문제를 처리할 수 있습니다.

표준 상용 Microsoft Azure 환경을 사용하지 않는 경우 Microsoft National Cloud Deployments 문서에서 Microsoft에서 운영하는 다양한 국가별 클라우드에 해당하는 Graph API 엔드포인트 목록을 참조하십시오.

단계 **1** Microsoft Intune에서 엔드포인트 인증을 위한 인증서를 구성합니다.

단계 **2** 조직의 요구 사항에 따라 다음 인증서 관리 프로토콜 중 하나와 해당 인증서 프로파일을 구성합니다.

- SCEP(Simple Certificate Enrollment Protocol)

1. Microsoft Intune을 사용하여 SCEP를 지원하도록 인프라를 구성합니다.
2. Microsoft Intune에서 SCEP 인증서 프로파일을 생성하고 할당합니다.

- 프라이빗 및 공개 키 인프라(PKI)

1. Microsoft Intune에서 PKCS 인증서를 구성하고 사용합니다.
2. PKCS 인증서 프로파일을 생성합니다.

참고 SCEP 또는 PKI 프로필을 구성할 때 **Subject Alternative Name(**주체 대체 이름**)** 영역에서 **Attribute(**특성**)**로 **URI**를 선택하고 **Value(**값**)**로 **ID:Microsoft Endpoint Manager:GUID:{{DeviceId}}**를 선택합니다.

단계 **3** Wi-Fi 프로파일을 생성하고 이전에 구성한 SCEP 또는 PKI 인증서 프로파일을 선택하여 **Subject Alternative Name(**주체 대체 이름**)** 필드에 GUID 값을 포함합니다.

Microsoft Intune에서 Wi-Fi 설정을 구성하는 방법에 대한 자세한 내용은 Microsoft Intune에서 디바이스에 Wi-Fi 설정 추가 및 사용을 참조하십시오.

Intune에서 VPN 서버에 연결하기 위해 VPN 프로파일을 생성하는 경우, Cisco ISE와 GUID 값을 공유할 인증서 기반 인증 유형을 선택해야 합니다.

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

Microsoft는 Azure AD(Azure Active Directory) Graph를 사용하지 않으며 2022년 6월 30일 이후에는 Azure AD Graph 지원 통합을 지원하지 않습니다. Azure AD Graph를 사용하는 모든 통합을 Microsoft Graph로 마이그레이션해야 합니다. Cisco ISE는 일반적으로 엔드포인트 관리 솔루션인 Microsoft Intune과의 통합을 위해 Azure AD Graph를 사용합니다. Azure AD Graph 애플리케이션 (https://graph.windows.net/<디렉터리*(*테넌트*)ID*>) 을 계속 사용하는 Cisco ISE와 Microsoft Intune 간의 통합은 2022년 6월 30일 이후에 작동하지 않습니다.

Azure AD Graph에서 Microsoft Graph로의 마이그레이션에 대한 자세한 내용은 다음 리소스를 참조하십시오.

- Azure AD Graph 앱을 Microsoft Graph로 마이그레이션
- Azure AD Graph에서 Microsoft Graph로의 마이그레이션 FAQ
- Microsoft 인증 라이브러리 및 Microsoft Graph API를 사용하도록 애플리케이션 업데이트

다음 Cisco ISE 릴리스는 Microsoft Graph 애플리케이션을 지원합니다.

- Cisco ISE 릴리스 2.7 패치 7

- Cisco ISE 릴리스 3.0 패치 5
- Cisco ISE 릴리스 3.1 패치 2

Cisco ISE를 지원되는 버전 중 하나로 업데이트한 후 Cisco ISE의 각 Microsoft Intune 서버 통합에서 **Auto Discovery URL(**자동 검색 **URL)** 필드를 수동으로 업데이트합니다(32단계).

https://graph.windows.net<디렉터리*(*테넌트*) ID*>를 **https://graph.microsoft.com**으로 대체합니다.

단계 **1** Microsoft Azure 포털에 로그인하고 **Azure Active Directory**로 이동합니다.

단계 **2** **Manage(**관리**)** > **App registrations(**앱 등록**)**를 선택합니다.

단계 **3** **New registration(**새 등록**)**을 클릭합니다.

단계 **4** 표시되는 **Register application(**애플리케이션 등록**)** 창에서 **Name(**이름**)** 필드에 값을 입력합니다.

단계 **5** **Supported Account Types(**지원되는 계정 유형**)** 영역에서 **Accounts in this organization directory only(**이 조직 디렉터리에만 있는 계정**)** 라디오 버튼을 클릭합니다.

단계 **6** **Register(**등록**)**를 클릭합니다.

새로 등록된 애플리케이션의 **Overview(**개요**)** 창이 표시됩니다. 이 창을 연 상태에서 Cisco ISE 관리 포털에 로그인합니다.

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

단계 **8** 표시된 인증서 목록에서 **Default self-signed server certificate(**기본 자체 서명 서버 인증서**)** 확인란을 선택하거나, 관리자 사용을 위해 구성한 다른 인증서 또는 옆에 있는 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** **View(**보기**)**를 클릭하여 이 인증서 세부 사항을 확인합니다. 표시된 **Certificate Hierarchy(**인증서 계층 구조**)** 대화 상자를 **Fingerprints(**핑거프린트**)** 영역으로 스크롤합니다. (이후 단계에서 이러한 값을 참조해야 합니다.)

단계 **12** Microsoft Azure Active Directory 포털의 왼쪽 창에서 **Certificates & secrets(**인증서 및 암호**)**를 클릭합니다.

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

단계 **14** 인증서가 업로드되면 창에 표시된 **Thumbprint(**지문**)** 값이 Cisco ISE 인증서의 **Fingerprint(**핑거프린트**)** 값과 일치하는지 확인합니다(11단계).

단계 **15** 왼쪽 창에서 **Manifest(**매니페스트**)**를 클릭합니다.

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

단계 **17** 왼쪽 창에서 **API permissions(API** 권한**)**를 클릭합니다.

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

API / 권한 이름	유형	설명
Intune		

API / 권한 이름	유형	설명
get_device_compliance	Application(애플리케이션)	Microsoft Intune에서 디바이스 상태 및 규정 준수 정보를 가져옵니다.
Microsoft Graph		
Directory.Read.All	Delegated(위임됨)	디렉터리 데이터를 읽습니다.
Directory.Read.All	Application(애플리케이션)	디렉터리 데이터를 읽습니다.
offline_access	Delegated(위임됨)	액세스 권한을 부여한 데이터에 대한 액세스를 유지합니다.
openid	Delegated(위임됨)	사용자로 로그인합니다.
User.Read	Delegated(위임됨)	사용자로 로그인하고 사용자 프로파일을 읽습니다.
User.Read.All	Delegated(위임됨)	모든 사용자의 전체 프로파일을 읽습니다.
User.Read.All	Application(애플리케이션)	모든 사용자의 전체 프로파일을 읽습니다.

단계 **19** 왼쪽 창에서 **API authorizations(API** 권한**)** > **Add a authorization(**사용 권한 추가**)** > **APIs my organization uses(**내 조직에서 사용하는 **API)**를 선택합니다.

단계 **20** **Windows Azure Active Directory**를 검색하고 검색 결과에서 동일한 항목을 선택합니다.

단계 **21** 다음 권한을 추가합니다.

API / 권한 이름	유형	설명
Azure Active Directory Graph		
Directory.Read.All	Delegated(위임됨)	디렉터리 데이터를 읽습니다.
Directory.Read.All	Application(애플리케이션)	디렉터리 데이터를 읽습니다.
User.Read.All	Delegated(위임됨)	모든 사용자의 전체 프로파일을 읽습니다.

권한을 추가한 후의 최종 테이블은 다음과 같아야 합니다.

그림 *3: Microsoft Intune*에서 구성해야 하는 *API* 및 권한

API / Permissions name	Type	Description	Admin consent requ...	Status
Azure Active Directory Graph (3)				
Directory.Read.All	Delegated	Read directory data	Yes	Granted
Directory.Read.All	Application	Read directory data	Yes	Granted
User.Read.All	Delegated	Read all users' full profiles	Yes	Granted
Intune (1)				
get_device_compliance	Application	Get device state and compliance information from Micros...	Yes	Granted
Microsoft Graph (7)				
Directory.Read.All	Delegated	Read directory data	Yes	Granted
Directory.Read.All	Application	Read directory data	Yes	Granted
offline_access	Delegated	Maintain access to data you have given it access to	No	Granted
openid	Delegated	Sign users in	No	Granted
User.Read	Delegated	Sign in and read user profile	No	Granted
User.Read.All	Delegated	Read all users' full profiles	Yes	Granted
User.Read.All	Application	Read all users' full profiles	Yes	Granted

단계 **22** ***<tenant name(***테넌트 이름***)>***에 대한 관리자 동의 부여를 클릭합니다.

단계 **23** 애플리케이션의 **Overview(**개요**)** 창에서 다음 세부 정보를 기록합니다.

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

단계 **24** **Overview(**개요**)** 창에서 **Endpoints(**엔드포인트**)**를 클릭하고 **Oauth 2.0 token endpoint (V2)(Oauth 2.0** 토큰 엔드포인트**(V2))** 필드의 값을 기록합니다.

단계 **25** https://fef.manage.microsoft.com/에서 PEM(체인) 형식으로 다음 인증서를 다운로드합니다.

- Baltimore CyberTrust 루트
- DigiCert SHA2 보안 서버 CA
- DigiCert 글로벌 루트 CA
- DigiCert 글로벌 루트 G2
- Microsoft Azure TLS 발급 CA 01
- Microsoft Azure TLS 발급 CA 02
- Microsoft Azure TLS 발급 CA 05
- Microsoft Azure TLS 발급 CA 06

Microsoft PKI 저장소에서 Microsoft Azure TLS 발급 CA 인증서를 다운로드할 수 있습니다.

참고 Microsoft Intune 인증서가 업데이트되었습니다. Microsoft Intune과 Cisco ISE 간의 성공적인 연결을 활성화하려면 새 루트 인증서를 가져와야 할 수 있습니다. Intune 인증서 업데이트: 연결을 계속하려면 작업이 필요할 수 있습니다.를 참조하십시오.

단계 **26** Cisco ISE 관리 포털에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Certificates(**인증서**)** > **Trusted Certificates(**신뢰할 수 있는 인증서**)**를 선택합니다.

단계 **27** 다운로드한 4개의 인증서 각각에 대해 다음 단계를 수행합니다.

1. **Import(**가져오기**)**를 클릭합니다.
2. **Choose File(**파일 선택**)**을 클릭하고 시스템에서 다운로드한 해당 인증서를 선택합니다.
3. 인프라 및 Cisco 서비스에서 사용할 수 있도록 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** 서비스의 인증 신뢰**)** 확인란을 선택합니다.
4. **Save(**저장**)**를 클릭합니다.

단계 **28** 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Network Resources(**네트워크 리소스**)** > **External MDM(**외부 **MDM)**을 선택합니다.

단계 **29** **Add(**추가**)**를 클릭합니다.

단계 **30** **Name(**이름**)** 필드에 값을 입력합니다.

단계 **31** **Authentication Type(**인증 유형**)** 드롭다운 목록에서 **OAuth** – **Client Credentials(OAuth** – 클라이언트 인증서**)**를 선택합니다.

단계 **32** 다음 필드에는 Microsoft Azure Active Directory에 있는 Microsoft Intune 애플리케이션의 정보가 필요합니다.

- **Auto Discovery URL(**자동 검색 **URL)** 필드에 **https://graph.microsoft.com/**<디렉터리*(*테넌트*) ID*>를 입력합니다.
- **Client ID(**클라이언트 **ID)** 필드에 Microsoft Intune 애플리케이션의 **Application (client) ID(**애플리케이션**(**클라이언트**) ID)** 값을 입력합니다.
- **Token Issuing URL(**토큰 발급 **URL)** 필드에 **Oauth 2.0** 토큰 엔드포인트**(V2)** 값을 입력합니다.
- **Token Audience(**토큰 대상**)** 필드에 **https://api.manage.microsoft.com/**을 입력합니다.

.

단계 **33** **Polling Interval(**폴링 간격**)** 및 **Time Interval For Compliance Device ReAuth Query(**컴플라이언스 디바이스 재인증 쿼리 시간 간격**)** 필드에 필요한 값을 입력합니다.

단계 **34** **Test Connection(**연결 테스트**)**을 클릭하여 Microsoft 서버에 연결할 수 있는지 확인합니다.

단계 **35** 연결 테스트에 성공하면 **Status(**상태**)** 드롭다운 목록에서 **Enabled(**활성화됨**)**를 선택합니다.

단계 **36** **Save(**저장**)**를 클릭합니다.

단계 **37** Cisco ISE 관리 포털에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Network Resources(**네트워크 리소스**)** > **External MDM(**외부 **MDM)**을 선택합니다. 추가된 Microsoft Intune 서버가 표시된 **MDM Server(MDM** 서버**)** 목록에 나타나야 합니다.

Ivanti(이전의 MobileIron) Unified Endpoint Management 서버 구성

참고 MobileIron은 Ivanti가 인수했습니다. MobileIron은 이 문서를 작성하는 시점에 MobileIron Core(온프레미스) 및 MobileIron Cloud와 같은 UEM(Unified Endpoint Management) 솔루션을 계속 제공합니다.

Cisco ISE 릴리스 3.1은 BasicAuth 프레임워크를 통해 API를 활용하여 MobileIron Core 또는 MobileIron Cloud 서버에 연결하고 이러한 서버에서 GUID 값을 수신합니다. 그런 다음 Cisco ISE는 MAC 주소 대신 GUID 값을 사용하여 엔드포인트를 식별하므로 MAC 주소 임의 설정이 사용 중일 때도 신뢰할 수 있는 인증이 가능합니다.

GUID 기반 인증은 X509 또는 ID 인증서라고도 하는 클라이언트 인증서를 사용하여 수행됩니다. GUID 값을 포함하도록 MobileIron Cloud 또는 MobileIron Core 서버에서 Cisco ISE로 보낸 인증서를 구성하려면 다음 작업을 수행하십시오.

MobileIron Core 11.3.0.0 빌드 24 이상 릴리스는 Cisco ISE에 대한 GUID 프로비저닝을 지원합니다.

MobileIron Cloud 또는 MobileIron Core 관리자 포털에서 다음 작업을 수행합니다.

1. 사용자 계정을 생성하고 필요한 API 권한을 할당합니다.
2. CA(Certificate Authority)를 구성합니다.
3. GUID 정보를 포함하도록 ID 인증서를 구성합니다.
4. 필요에 따라 루트 또는 신뢰할 수 있는 인증서를 업로드합니다.
5. Wi-Fi 프로파일을 구성합니다.

참고 이미 Cisco ISE 릴리스 3.1에 MobileIron Cloud 또는 MobileIron Core 서버를 연결하고 연결된 서버에서 GUID를 수신하려는 경우 필요에 따라 3, 4, 5 단계를 수행합니다.

기존 ID 인증서 또는 Wi-Fi 구성 또는 둘 다를 수정하는 경우 MobileIron은 업데이트된 구성을 연결된 매니지드 디바이스에 다시 게시합니다. MobileIron은 자체 서명 인증서 또는 로컬 CA의 사용을 권장하지 않습니다. 이 가이드에서는 Cisco ISE 릴리스 3.1에서 임의 및 변경 MAC 주소를 처리하는 데 필요한 주체 및 주체 대체 이름 속성 구성을 강조하기 위해 자체 서명 인증서 및 로컬 CA에 대한 단계를 예시로만 설명합니다.

Cisco ISE에서:

1. Cisco ISE의 MobileIron 포털에서 생성된 인증서를 업로드합니다.
2. MobileIron UEM 서버를 Cisco ISE에 연결합니다.

MobileIron Cloud UEM 서버 구성

다음 섹션은 더 큰 MobileIron Cloud UEM 서버 구성의 일부인 다양한 절차로 구성됩니다.

MobileIron Cloud 사용자 계정 생성 및 Cisco ISE 운영 역할 할당

단계 **1** MobileIron Cloud 포털에 로그인합니다.

단계 **2** 상단 메뉴에서 **Users(**사용자**)**를 선택합니다.

단계 **3** **Add(**추가**)** 드롭다운 메뉴에서 **Add API User(API** 사용자 추가**)**를 선택합니다.

단계 **4** **Add API User(API** 사용자 추가**)** 창에서 다음 필드의 값을 입력합니다.

- **Username(**사용자 이름**)**
- 이메일 주소
- 이름
- 성
- **Password(**비밀번호**)**
- 비밀번호 확인

단계 **5** 사용자가 Cisco ISE 통합에 필요한 API를 호출하도록 허용하려면 **Assign Roles(**역할 할당**)** 영역에서 **Cisco ISE Operations(Cisco ISE** 작업**)** 확인란을 선택합니다.

단계 **6** **Done(**완료**)**을 클릭합니다.

MobileIron Cloud에서 인증 기관 구성

이 절차에서는 로컬 CA를 구성하는 방법을 설명합니다. 그러나 MobileIron Cloud를 사용하면 광범위한 CA 구성 중에서 선택할 수 있습니다. 조직의 요구 사항에 가장 적합한 옵션을 선택합니다.

MobileIron Cloud에서 지원하는 다양한 유형의 인증서 관리에 대한 자세한 내용은 http://mi.extendedhelp.mobileiron.com/75/all/en/Welcome.htm#LocalCertificates.htm의 내용을 참조하십시오.

단계 **1** MobileIron Cloud 포털에서 **Admin(**관리**)** > **Certificate Management(**인증서 관리**)**를 선택합니다.

단계 **2** **Add(**추가**)**를 클릭합니다.

단계 **3** **Create a Standalone Certificate Authority(**독립형 인증 기관 생성**)**를 클릭합니다.

단계 **4** 표시되는 대화 상자에서 다음 필드에 세부 사항을 입력합니다.

1. **Name(**이름**)**
2. **Subject Parameters(**주체 매개 변수**)** 영역에서 다음 필드 중 하나 이상에 대한 값을 입력합니다.
   - 공용 이름

- 이메일
- 조직 단위
- 조직
- 도로 주소
- 시/군/구
- 지역
- 국가

3. **Key Generation Parameters(**키 생성 매개 변수**)** 영역에서 다음을 수행합니다.
   - **Key Type(**키 유형**)** 드롭다운 목록에서 **RSA**를 선택합니다.
   - **Signature Algorithm(**시그니처 알고리즘**)** 드롭다운 목록에서 **SHA256withRSA**를 선택합니다.
   - **Key Length(**키 길이**)** 드롭다운 목록에서 **2048**을 선택합니다.

MobileIron Cloud에서 루트 또는 신뢰할 수 있는 인증서 업로드

신뢰할 수 있는 서드 파티 CA를 사용하여 ID 인증서를 생성하는 경우 이 작업을 무시할 수 있습니다.

로컬 MobileIron Cloud CA 또는 회사 또는 조직에 전용인 내부 CA를 사용하는 경우 CA의 루트 인증서를 연결된 디바이스에 배포할 CA에 업로드해야 합니다. 이를 통해 디바이스는 인증에 사용되는 ID 인증서의 소스 또는 발급자를 신뢰할 수 있습니다.

단계 **1** MobileIron Cloud 메뉴에서 **Configurations(**구성**)**를 선택합니다.

단계 **2** **Add(**추가**)**를 클릭하고 **Certificate(**인증서**)**를 선택합니다.

단계 **3** **Name(**이름**)** 필드에 신뢰할 수 있는 인증서의 이름을 입력합니다.

단계 **4** **Configuration Setup(**구성 설정**)** 영역에서 **Choose File(**파일 선택**)**을 클릭하고 CA에 대한 신뢰할 수 있는 인증서 또는 루트 인증서를 선택합니다.

단계 **5** **Next(**다음**)**를 클릭합니다.

MobileIron Cloud에서 ID 인증서 구성

MobileIron Cloud에서 ID 인증서를 구성하여 모바일 디바이스용 인증서 인증 메커니즘을 정의합니다. ID 인증서는 X.509 인증서(.p12 또는 pfx 파일)입니다. 인증 기관을 소스로 사용하여 ID 인증서를 동적으로 생성할 수도 있습니다.

참고 Cisco ISE MDM 활용 사례에 대해 구성된 기존 ID 인증서가 MobileIron Cloud에 있는 경우 MobileIron 서버에서 GUID 정보를 수신하도록 이 절차의 5단계에 따라 인증서를 수정합니다.

단계 **1** MobileIron Cloud 메뉴에서 **Configurations(**구성**)**를 선택하고 **Identity Certificate(ID** 인증서**)**를 클릭합니다.

단계 **2** **Name(**이름**)** 필드에 값을 입력합니다.

단계 **3** **Configuration Setup(**구성 설정**)** 영역의 드롭다운 목록에서 **Dynamically Generated(**동적으로 생성됨**)**를 선택합니다.

단계 **4** **Source(**소스**)**드롭다운 목록에서 MobileIron Cloud에서 인증 기관 구성 절차에서 구성한 CA를 선택합니다.

단계 **5** **Subject Alternative Name Type(**주체 대체 이름 유형**)** 드롭다운 목록에서 **Uniform Resource Identifier**를 선택합니다.

단계 **6** **Subject Alternative Name Value(**주체 대체 이름 값**)** 필드에 **ID :Mobileiron:${deviceGUID}**를 입력합니다. GUID에 대한 Subject Alternative Name(주체 대체 이름) 필드를 구성하는 것이 좋습니다.

단계 **7** (선택 사항) 또는 Common Name(일반 이름) (CN) 필드를 사용하여 GUID를 Cisco ISE로 푸시하려면 **Subject(**제목**)** 필드에 **CN=ID:Mobileiron:${deviceGUID}**를 입력합니다.

단계 **8** **Test Configuration and Continue(**컨피그레이션 테스트 후 계속**)**를 클릭합니다.
Configuration Test Successful(컨피그레이션 테스트 성공**)** 대화 상자에 생성된 ID 인증서의 세부 사항이 표시됩니다.

단계 **9** **Distribute(**배포**)** 창에서 **Custom(**사용자 지정**)**을 클릭합니다.

단계 **10** **Define Device Group Distribution(**디바이스 그룹 배포 정의**)** 영역에서 이 구성에서 배포할 디바이스 그룹의 확인란을 선택합니다.

단계 **11** **Done(**완료**)**을 클릭합니다.

단계 **12** Cisco ISE MDM 활용 사례의 기존 ID 인증서에서 SAN 또는 CN 필드를 업데이트하는 경우 업데이트된 인증서를 네트워크에 연결된 최종 사용자에게 전송해야 합니다. 업데이트된 인증서를 최종 사용자에게 보내려면 **Configurations(**구성**)** > **Choose Config(**구성 선택**)** > **Edit(**편집**)** 창에서 **Clear cached certificates and issue new ones with recent updates(**캐시된 인증서를 지우고 최근 업데이트로 새 인증서를 발급합니다**)** 확인란을 선택합니다.

MobileIron Cloud에서 Wi-Fi 프로파일 구성

매니지드 iOS 및 Android 디바이스에 이미 Wi-Fi 프로파일을 구축한 경우 최신 ID 인증서 구성을 포함하도록 Wi-Fi 프로파일을 수정합니다. 그러면 연결된 디바이스는 Subject(주체) 또는 Subject Alternative Name(주체 대체 이름) 속성에 GUID가 포함된 새 ID 인증서를 수신합니다.

단계 **1** MobileIron Cloud 메뉴에서 **Configurations(**구성**)**를 선택하고 **Wi-Fi**를 클릭합니다.

단계 **2** **Name(**이름**)** 필드에 값을 입력합니다.

단계 **3** **SSID(Service Set Identifier)** 필드에 네트워크의 이름을 입력합니다.

단계 **4** **Auto Join(**자동 참가**)** 확인란은 기본적으로 선택되어 있습니다. 변경하지 마십시오.

단계 **5** **Security Type(**보안 유형**)** 드롭다운 목록에서 원하는 옵션을 선택합니다.

단계 **6** **Enterprise Settings(**엔터프라이즈 설정**)** 영역의 **Protocols(**프로토콜**)** 탭에서 **TLS** 확인란을 선택합니다.

단계 **7** **Authentication(**인증**)** 탭에서 **Username(**사용자 이름**)** 및 **Password(**비밀번호**)** 필드에 필요한 값을 입력합니다.

단계 **8** **Identity Certificate(ID** 인증서**)** 드롭다운 목록에서 절차 MobileIron Cloud에서 ID 인증서 구성, 14 페이지에서 생성한 ID 인증서를 선택합니다.

단계 **9** (선택 사항) **Trust(**신뢰**)** 탭에서 사용하려는 신뢰할 수 있는 인증서 옆의 확인란을 선택합니다.

단계 **10** **All Versions(**모든 버전**)** 영역의 **Network Type(**네트워크 유형**)** 드롭다운 목록에서 **Standard(**표준**)**를 선택합니다.

단계 **11** **Next(**다음**)**를 클릭합니다.

단계 **12** **Distribute(**배포**)** 창에서 필수 옵션을 클릭합니다.

단계 **13** **Define Device Group Distribution(**디바이스 그룹 배포 정의**)** 영역에서 이 구성에 포함할 디바이스 그룹 옆의 확인란을 선택합니다.

단계 **14** **Done(**완료**)**을 클릭합니다.

MobileIron Core UEM 서버 구성

다음 섹션은 더 큰 MobileIron Core UEM 서버 구성의 일부인 다양한 절차로 구성됩니다.

MobileIron Core 사용자 생성 및 API 권한 할당

단계 **1** MobileIron Core 관리자 포털에 로그인합니다.

단계 **2** **Devices and Users(**디바이스 및 사용자**)** > **Users(**사용자**)**를 선택합니다.

단계 **3** **Add(**추가**)** 드롭다운 메뉴에서 **Add Local User(**로컬 사용자 추가**)**를 선택합니다.

단계 **4** 다음 필드에 필요한 값을 입력합니다.

- 사용자 **ID**
- 이름
- 성
- **Password(**비밀번호**)**
- 비밀번호 확인
- 이메일

단계 **5** **Save(**저장**)**를 클릭합니다.

단계 **6** 새로 생성된 사용자에게 API 역할을 할당하려면 **Admin(**관리자**)**을 클릭하고 해당 사용자 이름 옆의 확인란을 선택합니다.

단계 **7** **Actions(**작업**)** 드롭다운 목록에서 **Assign to Space(**공간에 할당**)**를 선택합니다.

단계 **8** **Select Space(**공간 선택**)** 드롭다운 목록에서 사용자에 대해 사전 정의된 공간을 선택하거나 표시된 옵션에서 사용자에게 할당할 역할을 선택합니다. 생성한 사용자는 테넌트 관리자 권한이 있어야 하며, 이 사용자에 대해 **API** 역할이 활성화되어 있어야 합니다.

단계 **9** **Save(**저장**)**를 클릭합니다.

MobileIron Core에서 인증 기관 구성

MobileIron Core를 사용하면 광범위한 CA 구성 중에서 선택할 수 있습니다. 조직의 요구 사항에 가장 적합한 옵션을 선택합니다. 이 절차에서는 자체 서명 인증서에 대한 단계를 예로 들어 설명합니다.

단계 **1** MobileIron Core 관리자 포털에서 **Services(**서비스**)** > **Local CA(**로컬 **CA)**를 선택합니다.

단계 **2** **Add(**추가**)** 드롭다운 목록에서 **Generate Self-Signed Cert(**자체 서명 인증서 생성**)**를 선택합니다.

단계 **3** 표시되는 **Generate Self-Signed Certificate(**자체 서명 인증서 생성**)** 대화 상자에서 다음 필드에 필요한 값을 입력합니다.

- **Local CA Name(**로컬 **CA** 이름**)**
- **Key Length(**키 길이**)**
- **CSR Signature Algorithm(CSR** 서명 알고리즘**)**
- **Key Lifetime (in days)(**키 수명**(**일**))**
- **Issuer Name(**발급자 이름**)**

단계 **4** **Generate(**생성**)**를 클릭합니다.

단계 **5** 이후 단계에서 Cisco ISE에 이 인증서를 업로드해야 하므로 CA 인증서를 다운로드합니다. 다운로드할 인증서 옆에 있는 **View Certificate(**인증서 보기**)**를 클릭하고 표시되는 대화 상자에 모든 콘텐츠를 복사합니다. 선택한 텍스트 편집기에 이 콘텐츠를 붙여넣고 문서를 .cer 파일로 저장합니다.

MobileIron Core에서 루트 또는 신뢰할 수 있는 인증서 업로드

단계 **1** MobileIron Core 관리자 포털에서 **Policies and Configs(**정책 및 구성**)** > **Configurations(**구성**)**를 선택합니다.

단계 **2** **Add New(**새로 추가**)** 드롭다운 목록에서 **Certificates(**인증서**)**를 선택합니다.

단계 **3** 표시되는 **New Certificate Setting(**새 인증서 설정**)** 대화 상자에서 해당 필드에 인증서의 이름과 설명을 입력합니다.

단계 **4** **File Name(**파일 이름**)** 영역에서 **Browse(**찾아보기**)**를 클릭하고 이전에 구성한 CA에 대해 업로드해야 하는 루트 또는 신뢰할 수 있는 인증서를 선택합니다.

허용되는 파일 유형은 .cer, .crt, .pem 및 .der입니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

MobileIron Core에서 인증서 등록 구성

이 절차에서는 Cisco ISE 릴리스 3.1에서 임의 및 변경 MAC 주소를 처리하는 데 필요한 주체 및 주체 대체 이름 속성 구성을 강조 표시하기 위해 로컬 CA를 연결하는 단계를 예로 들어 설명합니다. MobileIron은 자체 서명 인증서 또는 로컬 CA의 사용을 권장하지 않습니다.

단계 **1** MobileIron Core 관리자 포털에서 **Policies and Configs(**정책 및 구성**)** > **Configurations(**구성**)**를 선택합니다.

단계 **2** **Add New(**새로 추가**)**를 클릭하고 **Certificate Enrollment(**인증서 등록**)**를 선택한 다음 구성한 CA에 적합한 커넥터를 선택합니다. 로컬 CA를 구성하는 경우 **Local(**로컬**)**을 선택합니다.

이 절차에서는 로컬 CA의 단계를 설명합니다. MobileIron Core 서버를 Cisco ISE에 연결하기 위해 구성한 CA에 따라 인증서 등록 옵션을 선택해야 합니다.

단계 **3** 표시되는 **New Local Certificate Enrollment Setting(**새 로컬 인증서 등록 설정**)** 대화 상자에서 다음 필드에 값을 제공합니다.

- 이름
- **Local CAs(**로컬 **CA)**
- **Key Type(**키 유형**)**
- **Subject(**제목**)**: **Subject(**제목**)** 필드를 사용하여 UUID(Cisco ISE에서는 GUID라고 함)를 Cisco ISE 3.1 이상 릴리스와 공유하려면 **CN=ID:Mobileiron:$DEVICE_UUID$**를 입력합니다.
- **Key Length(**키 길이**)**
- **CSR Signature Algorithm(CSR** 서명 알고리즘**)**
- **Subject Alternative Name Type(**주체 대체 이름 유형**)** 영역에서 **Add(**추가**)**를 클릭하고 **Type(**유형**)** 드롭다운 목록에서 **Uniform Resource Identifier**를 선택합니다. 이 필드를 사용하여 UUID(Cisco ISE에서는 GUID라고 함)를 Cisco ISE 3.1 이상 릴리스와 공유하려면 Value(값) 열에 **ID:Mobileiron:$DEVICE_UUID$**를 입력합니다.

단계 **4** **Issue Test Certificate(**테스트 인증서 발급**)**를 클릭합니다.

MobileIron Core에서 Wi-Fi 프로파일 구성

단계 **1** MobileIron Core 관리자 포털에서 **Policies and Configs(**정책 및 구성**)** > **Configurations(**구성**)**를 선택합니다.

단계 **2** **Add New(**새로 추가**)** 드롭다운 목록에서 **Wi-Fi**를 선택합니다.

단계 **3** **New Wi-Fi Setting(**새 **Wi-Fi** 설정**)** 대화 상자에서 다음 필드에 필요한 값을 입력합니다.

- **EAP Type(EAP** 유형**)**영역에서 **TLS** 확인란을 선택합니다.
- **Identity Certificate(ID** 인증서**)**드롭다운 목록에서 절차 MobileIron Core에서 인증서 등록 구성, 18 페이지에서 구성한 인증서 등록을 선택합니다.

- **Save(**저장**)**를 클릭합니다.

MobileIron Core의 레이블에 리소스 매핑

레이블을 구성하여 엔드포인트 및 디바이스 그룹에 적용해야 하는 구성, 규칙 및 프로파일을 정의합니다. 레이블을 사용하여 조직 단위, 디바이스 유형, 엔드포인트에서 실행 중인 운영 체제 등 다양한 기준에 따라 엔드포인트 및 디바이스를 그룹화할 수 있습니다. 레이블을 생성한 후 **Policies & Configs(**정책 및 구성**)** 창에서 이 레이블을 다양한 리소스에 할당하여 구성, 정책, 디바이스 또는 사용자 그룹을 서로 매핑합니다.

Cisco ISE 사용 사례에 대한 구성 및 정책을 매핑하고 배포하려면 적절한 레이블을 구성하고 인증서 등록, Wi-Fi 프로파일 및 이 사용 사례에 대해 생성한 기타 구성을 레이블에 적용합니다.

단계 **1** 레이블 생성:

1. MobileIron Core 관리자 포털에서 **Devices & Users(**디바이스 및 사용자**)** > **Labels(**레이블**)**를 선택합니다.
2. **Add Label(**라벨 추가**)**을 클릭합니다.
3. **Add Label(**레이블 추가**))** 대화 상자에서 **Name(**이름**)** 필드에 레이블의 이름을 입력합니다.
4. **Criteria(**기준**)** 영역에서 **Field(**필드**)**, **Operator(**연산자**)** 및 **Value(**값**)** 필드에서 적절한 값을 선택하여 이 레이블의 매개변수를 정의합니다.
5. **Save(**저장**)**를 클릭합니다.

단계 **2** **Policies & Configs(**정책 및 구성**)** 리소스에 레이블을 할당합니다.

1. MobileIron Core 관리자 포털에서 **Policies & Configs(**정책 및 구성**)**를 클릭하고 원하는 리소스 메뉴를 선택합니다.
2. 생성한 레이블을 할당할 구성 또는 정책의 확인란을 선택합니다.
3. **Actions(**작업**)** 드롭다운 목록에서 **Apply To Label(**레이블에 적용**)**을 선택합니다.
4. **Apply To Label(**레이블에 적용**)** 대화 상자에서 적용할 레이블 옆의 확인란을 선택하고 **Apply(**적용**)**를 클릭합니다.

추가 참조 자료

다음 링크에는 Cisco ISE로 작업할 때 사용할 수 있는 추가 리소스가 포함되어 있습니다.https://www.cisco.com/c/en/us/td/docs/security/ise/end-user-documentation/Cisco_ISE_End_User_Documentation.html

통신, 서비스 및 추가 정보

- Cisco에서 시기에 맞는 관련된 정보를 받으려면 Cisco Profile Manager에 로그인합니다.
- 중요한 기술로 원하는 비즈니스 결과를 얻으려면 Cisco Services를 참조하십시오.
- 서비스 요청을 제출하려면 Cisco 지원을 참조하십시오.
- 안전하고 검증된 엔터프라이즈급 앱, 제품, 솔루션 및 서비스를 검색하고 찾아보려면 Cisco DevNet을 참조하십시오.
- 일반 네트워킹, 교육 및 인증서 제목을 얻으려면 Cisco Press를 참조하십시오.
- 특정 제품 또는 제품군에 대한 보증 정보를 찾으려면 Cisco Warranty Finder에 액세스합니다.

Cisco Bug Search Tool

Cisco BST(Bug Search Tool)는 Cisco 제품 및 소프트웨어에 있는 결함 및 취약점의 종합적인 목록을 유지관리하는 Cisco 버그 추적 시스템에 대한 게이트웨이입니다. BST에서는 제품 및 소프트웨어에 대한 자세한 결함 정보를 제공합니다.

문서 피드백

Cisco 기술 문서에 대한 피드백을 제공하려면 모든 온라인 문서의 오른쪽 창에 있는 피드백 양식을 사용하십시오.