자산 가시성

외부 ID 저장소를 사용하는 Cisco ISE에 대한 관리 액세스

Cisco ISE에서 Active Directory, LDAP 또는 RSA SecureID와 같은 외부 ID 저장소를 통해 관리자를 인증할 수 있습니다. 외부 ID 저장소를 통해 인증을 제공하는 데 사용할 수 있는 두 가지 모델이 있습니다.

- 외부 인증 및 권한 부여: 관리자를 위해 로컬 Cisco ISE 데이터베이스에 지정된 자격 증명이 없으며, 권한 부여는 외부 ID 저장소 그룹 멤버십만을 기반으로 합니다. 이 모델은 Active Directory 및 LDAP 인증에 사용됩니다.
- 외부 인증 및 내부 권한 부여: 관리자의 인증 자격 증명은 외부 ID 소스에서 가져오며, 권한 부여 및 관리자 역할 할당은 로컬 Cisco ISE 데이터베이스를 사용하여 발생합니다. 이 모델은 RSA SecurID 인증에 사용됩니다. 이 방법을 사용하려는 경우 외부 ID 저장 및 현지 Cisco ISE 데이터베이스에서 모두 동일한 사용자 이름을 구성해야 합니다.

Cisco ISE는 인증 프로세스 중에 외부 ID 저장소와의 통신이 설정되지 않았거나 통신이 실패할 경우 "대체"되어 내부 ID 데이터베이스에서 인증하려고 시도하도록 설계되었습니다. 또한 외부 인증을 설정한 관리자가 브라우저를 실행하고 로그인 세션을 시작하는 경우에도 여전히 관리자는 로그인 대화 상자의 **Identity Store(ID** 저장소**)** 드롭다운 목록에서 **Internal(**내부**)**을 선택하여 Cisco ISE 로컬 데이터베이스를 통해 인증을 요청할 수 있습니다.

슈퍼 관리자 그룹에 속하고 외부 ID 저장소를 사용하여 인증하고 권한을 부여하도록 구성된 관리자는 외부 ID 저장소로 인증하여 CLI(command-line interface) 액세스할 수도 있습니다.

참고 관리자 포털을 통해서만 외부 관리자 인증을 제공하는 이 방법을 구성할 수 있습니다. Cisco ISE CLI는 이러한 기능을 제공하지 않습니다.

네트워크에 하나 이상의 기존 외부 ID 저장소가 없는 경우 필요한 외부 ID 저장소를 설치하고 그러한 ID 저장소에 액세스하도록 Cisco ISE를 구성했는지 확인합니다.

외부 인증 및 권한 부여

기본적으로 Cisco ISE는 내부 관리자 인증을 제공합니다. 외부 인증을 설정하려면 외부 ID 저장소에 정의하는 외부 관리자 계정에 대한 비밀번호 정책을 생성해야 합니다. 그런 다음 이 정책을 외부 관리자 그룹에 적용할 수 있습니다. 그 결과 해당 정책은 외부 관리자 RBAC 정책에 포함됩니다.

외부 인증을 구성하려면 다음을 수행해야 합니다.

- 외부 ID 저장소를 사용하여 비밀번호 기반 인증을 구성합니다.
- 외부 관리자 그룹을 생성합니다.
- 메뉴 액세스 및 외부 관리자 그룹에 대한 데이터 액세스 권한을 구성합니다.
- 외부 관리자 인증을 위한 RBAC 정책을 생성합니다.

외부 ID 저장소를 통해 인증을 제공하는 것 외에 네트워크에서 CAC(Common Access Card) 인증 디바이스를 사용해야 할 수도 있습니다.

외부 **ID** 저장소를 사용하여 비밀번호 기반 인증 구성

Active Directory 또는 LDAP 등의 외부 ID 저장소를 사용하여 인증하는 관리자에 대해 먼저 비밀번호 기반 인증을 구성해야 합니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Admin Access(**관리자 액세스**)** > **Authentication(**인증**)**을 선택합니다.

단계 **2** **Authentication Method(**인증 방법**)** 탭에서 **Password Based(**비밀번호 기반**)**를 클릭하고 이미 구성한 외부 ID 소스 중 하나를 선택합니다. 예를 들어 직접 생성한 Active Directory 인스턴스를 선택할 수 있습니다.

단계 **3** 외부 ID 저장소를 사용하여 인증하는 관리자에 대해 적용하려는 기타 특정 비밀번호 기반 정책 설정을 구성합니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

외부 관리자 그룹 생성

외부 Active Directory 또는 LDAP 관리자 그룹을 생성해야 합니다. 그러면 Cisco ISE가 외부 Active Directory 또는 LDAP ID 저장소에 정의되어 있는 사용자 이름을 사용하여 로그인 시 사용자가 입력하는 관리자 사용자 이름 및 비밀번호를 검증합니다.

Cisco ISE는 외부 리소스에서 Active Directory 또는 LDAP 그룹 정보를 가져온 다음 사전 속성으로 저장합니다. 이러한 외부 관리자 인증 방법에 대해 RBAC 정책을 구성하는 동안 정책 구성 요소 중 하나로 해당 속성을 지정할 수 있습니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Admin Access(**관리자 액세스**)** > **Administrators(**관리자**)** > **Admin Groups(**관리자 그룹**)**를 선택합니다.

External Groups Mapped(외부 그룹 매핑됨**)** 열에 내부 RBAC 역할에 매핑된 외부 그룹 수가 표시됩니다. 관리자 역할에 해당하는 번호를 클릭하여 외부 그룹을 볼 수 있습니다. 예를 들어 Super Admin(슈퍼 관리자)에 대해 2를 클릭하면 두 개의 외부 그룹 이름이 표시됩니다.

단계 **2** **Add(**추가**)**를 클릭합니다.

단계 **3** 이름과 설명(선택 사항)을 입력합니다.

단계 **4** **External(**외부**)**을 클릭합니다.

Active Directory 도메인에 연결하고 조인한 경우에는 Active Directory 인스턴스 이름이 **Name(**이름**)** 필드에 표시됩니다.

단계 **5** **External Groups(**외부 그룹**)** 드롭다운 목록 상자에서 이 외부 관리자 그룹에 매핑할 Active Directory 그룹을 선택합니다.

"+" 기호를 클릭하여 추가 Active Directory 그룹을 이 외부 관리자 그룹에 매핑합니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

내부 읽기 전용 관리자 생성

단계 **1** **Administration(**관리**)** > **System(**시스템**)** > **Admin Access(**관리자 액세스**)** > **Administrators(**관리자**)** > **Admin Users(**관리 사용자**)**Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 .

단계 **2** **Add(**추가**)**를 클릭하고 **Create An Admin User(**관리 사용자 생성**)**를 선택합니다.

단계 **3** 읽기 전용 관리자를 생성하려면 **Read Only(**읽기 전용**)** 확인란을 선택합니다.

읽기 전용 관리자 그룹에 외부 그룹 매핑

단계 **1** 외부 인증 소스를 구성하려면 **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **External Identity Sources(**외부 **ID** 소스**)**Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 .

단계 **2** 필요한 외부 ID 소스(예: Active Directory 또는 LDAP)를 클릭한 다음 선택한 ID 소스에서 그룹을 검색합니다.

단계 **3** 관리자 액세스의 인증 방법을 ID 소스와 매핑하려면 **Administration(**관리**)** > **System(**시스템**)** > **Admin Access(**관리자 액세스**)** > **Authentication(**인증**)**을 선택합니다.

단계 **4** **Administration(**관리**)** > **System(**시스템**)** > **Admin Access(**관리자 액세스**)** > **Administrators(**관리자**)** > **Admin Groups(**관리자 그룹**)**를 선택한 다음 **Read Only Admin(**읽기 전용 관리자**)** 그룹을 선택합니다.

단계 **5** **External(**외부**)** 확인란을 선택하고 읽기 전용 권한을 제공해야 할 외부 그룹을 선택합니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

읽기 전용 관리자 그룹에 매핑된 외부 그룹은 다른 관리자 그룹에 할당할 수 없습니다.

외부 관리자 그룹에 대한 메뉴 액세스 및 데이터 액세스 권한 구성

외부 관리자 그룹에 할당할 수 있는 메뉴 액세스 및 데이터 액세스 권한을 구성해야 합니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 를 선택합니다.

단계 **2** 다음 중 하나를 클릭합니다.

- **Menu Access(**메뉴 액세스**)**: 외부 관리자 그룹에 속하는 모든 관리자에게 메뉴 또는 하위 메뉴 레벨에서 권한을 부여할 수 있습니다. 메뉴 액세스 권한에 따라 관리자가 액세스할 수 있는 메뉴 또는 하위 메뉴가 결정됩니다.
- **Data Access(**데이터 액세스**)**: 외부 관리자 그룹에 속하는 모든 관리자에게 데이터 레벨에서 권한을 부여할 수 있습니다. 데이터 액세스 권한에 따라 관리자가 액세스할 수 있는 데이터가 결정됩니다.

단계 **3** 외부 관리자 그룹에 대한 메뉴 액세스 또는 데이터 액세스 권한을 지정합니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

외부 관리자 인증을 위한 **RBAC** 정책 생성

외부 ID 저장소를 사용하여 관리자를 인증하는 동시에 사용자 맞춤화 메뉴 및 데이터 액세스 권한을 지정하려면 새 RBAC 정책을 구성해야 합니다. 이 정책은 외부 인증 및 권한 부여를 관리하기 위한 Cisco ISE 메뉴 및 데이터 액세스 권한과 인증용 외부 관리자 그룹을 포함해야 합니다.

참고 기존의 시스템 사전 설정 RBAC 정책을 수정하여 이러한 새 외부 속성을 지정할 수는 없습니다. 템플릿으로 사용하려는 기존 정책이 있는 경우에는 해당 정책을 복제하고 이름을 바꾼 후에 새 속성을 할당해야 합니다.

단계 **1** **Administration(**관리**)** > **System(**시스템**)** > **Admin Access(**관리자 액세스**)** > **Authorization(**권한 부여**)** > **RBAC Policy(RBAC** 정책**)**Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 .

단계 **2** 규칙 이름, 외부 관리자 그룹 및 권한을 지정합니다.

적절한 외부 관리자 그룹을 올바른 관리자 사용자 ID에 할당해야 합니다. 관리자가 올바른 외부 관리자 그룹에 연결되어 있는지 확인합니다.

단계 **3** **Save(**저장**)**를 클릭합니다.

관리자로 로그인하는 경우 Cisco ISE RBAC 정책이 관리자 ID를 인증할 수 없으면 Cisco ISE에 "인증되지 않음" 메시지가 표시되며 관리 포털에 액세스할 수 없습니다.

내부 권한 부여를 사용하는 인증을 위해 외부 **ID** 저장소를 사용하여 관리자 액세스 구성

이 방법을 사용하려는 경우 외부 ID 저장 및 현지 Cisco ISE 데이터베이스에서 모두 동일한 사용자 이름을 구성해야 합니다. Cisco ISE가 외부 RSA SecurID ID 저장소를 사용하여 관리자 인증을 제공하도록 구성하면 RSA ID 저장소에 의해 관리자 자격 증명 인증이 수행됩니다. 그러나 권한 부여(정책 적용)는 계속해서 Cisco ISE 내부 데이터베이스에 따라 수행됩니다. 또한 외부 인증 및 권한 부여와는 다른 두 가지 중요한 요소가 있습니다.

- 관리자에 대해 특정 외부 관리자 그룹을 지정하지 않아도 됩니다.
- 외부 ID 저장소와 로컬 Cisco ISE 데이터베이스 둘 다에서 같은 사용자 이름을 구성해야 합니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Admin Access(**관리자 액세스**)** > **Administrators(**관리자**)** > **Admin Users(**관리 사용자**)**를 선택합니다.

단계 **2** 외부 RSA ID 저장소의 관리 사용자 이름이 Cisco ISE에도 있는지 확인합니다. Password(비밀번호) 아래에서 **External(**외부**)** 옵션을 클릭해야 합니다.

참고 이 외부 관리자 사용자 ID에 대해서는 비밀번호를 지정할 필요가 없으며 구체적으로 구성된 외부 관리자 그룹을 연결된 RBAC 정책에 적용할 필요도 없습니다.

단계 **3** **Save(**저장**)**를 클릭합니다.

외부 인증 프로세스 플로우

관리자가 로그인하면 로그인 세션은 프로세스의 다음 단계를 거칩니다.

1. 관리자는 RSA SecurID 시도를 보냅니다.
2. RSA SecurID가 시도 응답을 반환합니다.
3. 관리자가 사용자 ID와 비밀번호를 입력하는 것처럼 Cisco ISE 로그인 대화 상자에 사용자 이름 및 RSA SecurID 시도 응답을 입력합니다.
4. 관리자가 지정된 ID 저장소가 외부 RSA SecurID 리소스인지 확인합니다.
5. 관리자가 **Login(**로그인**)**을 클릭합니다.

로그인되면 관리자에게는 메뉴 및 RBAC 정책에 지정된 데이터 액세스 항목만 표시됩니다.

외부 **ID** 소스

이러한 창에서는 Cisco ISE가 인증 및 권한 부여에 사용하는 사용자 데이터가 포함되어 있는 외부 ID 소스를 구성하고 관리할 수 있습니다.

LDAP ID 소스 설정

다음 표에서는 LDAP 인스턴스를 생성하고 해당 인스턴스에 연결하는 데 사용할 수 있는 LDAP ID 소스 창의 필드에 대해 설명합니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **External Identity Sources(**외부 **ID** 소스**)** > **LDAP**입니다.

LDAP 일반 설정

다음 표에서는 **General(**일반**)** 탭의 필드에 대해 설명합니다.

표 ***1: LDAP*** 일반 설정

필드 이름	사용 지침
Name(이름**)**	LDAP 인스턴스 이름을 입력합니다. 이 값은 검색에서 주체 DN 및 속성을 가져오는 데 사용됩니다. 값은 문자열 유형이며 최대 길이는 64자입니다.
Description(설명**)**	LDAP 인스턴스에 대한 설명을 입력합니다. 이 값은 문자열 유형이며 최대 길이는 1,024자입니다.

필드 이름	사용 지침
Schema(스키마**)**	다음과 같은 내장 스키마 유형 중 하나를 선택하거나 사용자 맞춤화 스키마를 생성할 수 있습니다. • Active Directory • Sun Directory 서버 • Novell eDirectory Schema(스키마) 옆의 화살표를 클릭하여 스키마 세부정보를 확인할 수 있습니다. 사전 정의된 스키마의 속성을 편집하면 Cisco ISE가 자동으로 사용자 맞춤화 스키마를 생성합니다.
참고 다음 필드는 사용자 맞춤화 스키마를 선택할 때만 편집할 수 있습니다.	
Subject Objectclass	검색에서 주체 DN 및 속성을 가져오기 위해 사용할 값을 입력합니다. 값은 문자열 유형이며 최대 길이는 256자입니다.
Subject Name Attribute(주체 이름 속성**)**	요청의 사용자 이름이 포함된 속성의 이름을 입력합니다. 값은 문자열 유형이며 최대 길이는 256자입니다.
Group Name Attribute(그룹 이름 속성**)**	• CN: 공용 이름을 기준으로 LDAP ID 저장소 그룹을 검색하려는 경우 입력합니다. • DN: 고유 이름을 기준으로 LDAP ID 저장소 그룹을 검색하려는 경우 입력합니다.
Certificate Attribute(인증서 속성**)**	인증서 정의를 포함하는 속성을 입력합니다. 인증서 기반 인증의 경우 이러한 정의는 클라이언트가 제공하는 인증서를 검증하는 데 사용됩니다.
Group Objectclass	검색에서 그룹으로 인식되는 객체를 지정하기 위해 사용할 값을 입력합니다. 값은 문자열 유형이며 최대 길이는 256자입니다.
Group Map Attribute(그룹 맵 속성**)**	매핑된 정보를 포함하는 속성을 지정합니다. 이 속성은 선택한 참조 방향에 따라 사용자 또는 그룹 속성일 수 있습니다.
Subject Objects Contain Reference To Groups(주체 객체가 그룹에 대한 참조를 포함함**)**	주체 객체가 속한 그룹을 지정하는 속성이 주체 객체에 포함되어 있으면 이 옵션을 클릭합니다.

필드 이름	사용 지침
Group Objects Contain Reference To Subjects(그룹 객체가 주체에 대한 참조를 포함함**)**	그룹 객체가 주체를 지정하는 속성을 포함하고 있으면 이 옵션을 클릭합니다. 이 값이 기본값입니다.
Subjects in Groups Are Stored in Member Attribute As(그룹의 주체가 멤버 속성에 다른 이름으로 저장됨**)**	(**Group Objects Contain Reference To Subjects(**그룹 객체가 주체에 대한 참조를 포함함**)** 옵션을 활성화하는 경우에만 사용 가능함) 그룹 멤버 속성에서 멤버가 제공되는 방법을 지정하며, 기본값은 DN입니다.
User Info Attributes(사용자 정보 속성**)**	기본적으로, 사전 정의된 속성은 다음과 같은 내장 스키마 유형에 대한 사용자 정보(예: 이름, 성, 이메일, 전화 번호, 소재지 등)를 수집하는 데 사용됩니다. • Active Directory • Sun Directory 서버 • Novell eDirectory 사전 정의된 스키마의 속성을 편집하면 Cisco ISE가 자동으로 사용자 맞춤화 스키마를 생성합니다. 스키마 드롭다운 목록에서 Custom(사용자 맞춤화) 옵션을 선택하여 요건에 따라 사용자 정보 속성을 편집할 수도 있습니다.

LDAP 연결 설정

다음 표에서는 **Connection Settings(**연결 설정**)** 탭의 필드에 대해 설명합니다.

표 ***2: LDAP*** 연결 설정

필드 이름	사용 지침
Enable Secondary Server(보조 서버 활성화**)**	기본 LDAP 서버에서 장애가 발생하는 경우 백업으로 사용할 보조 LDAP 서버를 활성화하려면 이 옵션을 선택합니다. 이 확인란을 선택하는 경우 보조 LDAP 서버에 대한 컨피그레이션 매개변수를 입력해야 합니다.
Primary and Secondary Servers(기본 서버 및 보조 서버**)**	

필드 이름	사용 지침
Hostname/IP(호스트 이름**/IP)**	LDAP 소프트웨어를 실행 중인 머신의 IP 주소 또는 DNS 이름을 입력합니다. 호스트 이름은 1~256자로 입력하거나 문자열로 표시되는 유효한 IP 주소를 포함할 수 있습니다. 호스트 이름에 사용할 수 있는 문자는 영숫자 문자(a~z, A~Z, 0~9)와 점(.), 하이픈(-)입니다.
Port(포트**)**	LDAP 서버가 수신 대기 중인 TCP/IP 포트 번호를 입력합니다. 유효한 값은 1~65,535입니다. 기본값은 LDAP 사양에 나와 있는 389입니다. 포트 번호를 모르는 경우 LDAP 서버 관리자에서 이 정보를 찾을 수 있습니다.
Specify server for each ISE node(각 **ISE** 노드에 대한 서버 지정**)**	각 PSN에 대해 기본 및 보조 LDAP 서버 호스트 이름/IP 및 해당 포트를 구성하려면 이 확인란을 선택합니다. 이 옵션을 활성화하면 구축의 모든 노드를 나열하는 표가 표시됩니다. 노드를 선택하고 선택한 노드에 대한 기본 및 보조 LDAP 서버 호스트 이름/IP 및 해당 포트를 구성해야 합니다.
Access(액세스**)**	**Anonymous Access(**익명 액세스**)**: LDAP 디렉토리의 검색이 익명으로 수행되도록 하려면 클릭합니다. 이 경우 서버는 클라이언트를 구분하지 않으며, 인증되지 않은 클라이언트가 액세스할 수 있도록 구성된 모든 데이터에 대한 읽기 권한을 클라이언트에 허용합니다. 서버로 인증 정보를 전송하도록 허용하는 특정 정책이 없는 경우 클라이언트는 익명 연결을 사용해야 합니다. **Authenticated Access(**인증된 액세스**)**: LDAP 디렉토리의 검색이 관리 자격 증명을 사용하여 수행되도록 하려면 클릭합니다. 이 설정을 클릭하는 경우 Admin DN(관리자 DN) 및 Password(비밀번호) 필드에 정보를 입력합니다.
Admin DN(관리자 **DN)**	관리자의 DN을 입력합니다. 관리자 DN은 사용자 디렉토리 서브트리에서 필요한 모든 사용자 및 그룹을 검색할 권한이 있는 LDAP 계정입니다. 지정된 관리자에게 검색에서 그룹 이름 속성을 확인할 권한이 없으면 해당 LDAP 서버에 의해 인증된 사용자에 대한 그룹 매핑이 실패합니다.
Password(비밀번호**)**	LDAP 관리자 계정 비밀번호를 입력합니다.

필드 이름	사용 지침
Secure Authentication(보안 인증**)**	SSL을 사용하여 Cisco ISE와 기본 LDAP 서버 간의 통신을 암호화하려면 클릭합니다. Port(포트) 필드에 LDAP 서버의 SSL에 사용되는 포트 번호가 포함되어 있는지 확인합니다. 이 옵션을 활성화하는 경우 루트 CA를 선택해야 합니다.
LDAP Server Root CA(LDAP 서버 루트 **CA)**	인증서를 사용한 보안 인증을 활성화하려면 드롭다운 목록에서 신뢰할 수 있는 루트 인증 기관을 선택합니다.
Server Timeout(서버 시간 초과**)**	기본 LDAP 서버와의 연결이나 인증이 실패했다고 결정할 때까지 Cisco ISE가 해당 서버로부터의 응답을 대기할 시간을 초 단위로 입력합니다. 유효한 값은 1~99입니다. 기본값은 10입니다.
Max. Admin Connections(최대 관리자 연결 수**)**	특정 LDAP 컨피그레이션에 대해 실행할 수 있는 LDAP 관리자 계정 권한이 있는 최대 동시 연결 수(0보다 큼)를 입력합니다. 이러한 연결은 디렉토리 검색 시 사용자 디렉토리 서브트리 및 그룹 디렉토리 서브트리에서 사용자와 그룹을 검색하는 데 사용됩니다. 유효한 값은 1~99입니다. 기본값은 20입니다.
Force reconnect every N seconds(N초마다 강제로 다시 연결**)**	서버가 지정된 시간 간격에 LDAP 연결을 갱신하도록 강제 지정하려면 이 확인란을 선택하고 **Seconds(**초**)** 필드에 원하는 값을 입력합니다. 유효 범위는 1분~60분입니다.
Test Bind to Server(서버에 대한 바인딩 테스트**)**	LDAP 서버 세부정보 및 자격 증명을 정상적으로 바인딩할 수 있는지를 테스트하고 확인하려면 클릭합니다. 테스트가 실패하는 경우 LDAP 서버 세부정보를 편집한 후에 다시 테스트해 주십시오.
Failover(페일오버**)**	
Always Access Primary Server First(항상 기본 서버에 먼저 액세스**)**	Cisco ISE가 인증 및 권한 부여를 위해 항상 기본 LDAP 서버에 먼저 액세스하도록 하려면 이 옵션을 클릭합니다.
Failback to Primary Server After(다음 시간 이후 기본 서버로 장애 복구**)**	Cisco ISE가 연결하려고 하는 기본 LDAP 서버에 연결할 수 없는 경우 Cisco ISE는 보조 LDAP 서버에 연결하려고 시도합니다. Cisco ISE가 기본 LDAP 서버를 다시 사용하도록 하려면 이 옵션을 클릭하고 텍스트 상자에 값을 입력합니다.

LDAP 디렉토리 조직 설정

다음 표에서는 **Directory Organization(**디렉토리 조직**)** 탭의 필드에 대해 설명합니다.

표 ***3: LDAP*** 디렉토리 조직 설정

필드 이름	사용 지침
Subject Search Base(주체 검색 기준**)**	모든 주체를 포함하는 서브트리의 DN을 입력합니다. 예를 들면 다음과 같습니다. o=corporation.com 주체를 포함하는 트리가 기본 DN인 경우 LDAP 컨피그레이션에 따라 o=corporation.com 또는 dc=corporation,dc=com 을 입력합니다. 자세한 내용은 LDAP 데이터베이스 설명서를 참고해 주십시오.
Group Search Base(그룹 검색 기준**)**	모든 그룹을 포함하는 서브트리의 DN을 입력합니다. 예를 들면 다음과 같습니다. ou=조직 단위, ou=다음 조직 단위, o=corporation.com 그룹을 포함하는 트리가 기본 DN인 경우 LDAP 컨피그레이션에 따라 o=corporation.com 또는 dc=corporation,dc=com 을 입력합니다. 자세한 내용은 LDAP 데이터베이스 설명서를 참고해 주십시오.

필드 이름	사용 지침
Search for MAC Address in Format(MAC 주소 검색 형식**)**	LDAP 데이터베이스에서 Cisco ISE가 검색에 사용할 MAC 주소 형식을 입력합니다. 내부 ID 소스의 MAC 주소는 xx-xx-xx-xx-xx-xx 형식으로 제공됩니다. LDAP 데이터베이스의 MAC 주소는 다른 형식으로 제공될 수 있습니다. 그러나 Cisco ISE는 호스트 조회 요청을 받으면 MAC 주소를 내부 형식에서 이 필드에 지정된 형식으로 변환합니다. 드롭다운 목록을 사용하여 특정 형식의 MAC 주소 검색을 활성화합니다. 여기서 <*format*>은 다음 중 하나일 수 있습니다. • xxxx.xxxx.xxxx • xxxxxxxxxxxx • xx-xx-xx-xx-xx-xx • xx:xx:xx:xx:xx:xx 선택한 형식은 LDAP 서버에서 제공되는 MAC 주소의 형식과 일치해야 합니다.
Strip Start of Subject Name Up To the Last Occurrence of the Separator(마지막으로 나타나는 구분 기호까지 주체 이름 시작 부분 분리**)**	사용자 이름에서 도메인 접두사를 제거하려면 적절한 텍스트를 입력합니다. Cisco ISE는 사용자 이름에서 이 필드에 지정된 구분 기호 문자를 찾으면 사용자 이름이 시작되는 부분부터 구분 기호 문자까지의 모든 문자를 분리합니다. <start_string> 상자에 지정된 문자 중 두 개 이상이 사용자 이름에 포함되어 있으면 Cisco ISE는 마지막으로 나타나는 구분 기호까지 문자를 분리합니다. 예를 들어 구분 기호 문자가 백슬래시(\)이고 사용자 이름이 DOMAIN\user1이면 Cisco ISE는 user1을 LDAP 서버에 제출합니다. 참고 <start_string>은 우물 정자(#), 물음표(?), 큰따옴표("), 별표(*), 오른쪽 꺾쇠 괄호(>) 및 왼쪽 꺾쇠 괄호(<)와 같은 특수 문자를 포함할 수 없습니다. Cisco ISE에서는 사용자 이름에 이러한 문자를 사용할 수 없습니다.

필드 이름	사용 지침
Strip End of Subject Name from the First Occurrence of the Separator(처음으로 나타나는 구분 기호부터 주체 이름 끝 부분 분리**)**	사용자 이름에서 도메인 접미사를 제거하려면 적절한 텍스트를 입력합니다. Cisco ISE는 사용자 이름에서 이 필드에 지정된 구분 기호 문자를 찾으면 구분 기호 문자부터 사용자 이름이 끝나는 부분까지의 모든 문자를 분리합니다. 이 필드에 지정된 문자 중 두 개 이상이 사용자 이름에 포함되어 있으면 Cisco ISE는 처음으로 나타나는 구분 기호부터 문자를 분리합니다. 예를 들어 구분 기호 문자가 @이고 사용자 이름이 *user1@domain*이면 Cisco ISE는 *user1*을 LDAP 서버에 제출합니다. 참고 <*end_string*> 상자에는 우물 정자(#), 물음표(?), 큰따옴표("), 별표(*), 오른쪽 꺾쇠 괄호(>) 및 왼쪽 꺾쇠 괄호(<)와 같은 특수 문자를 포함할 수 없습니다. Cisco ISE에서는 사용자 이름에 이러한 문자를 사용할 수 없습니다.

LDAP 그룹 설정

표 ***4: LDAP*** 그룹 설정

필드 이름	사용 지침
Add(추가**)**	새 그룹을 추가하려면 **Add(**추가**) > Add Group(**추가 그룹**)**을 선택합니다. 또는 LDAP 디렉토리에서 그룹을 선택하려면 **Add(**추가**) > Select Groups From Directory(**디렉토리에서 그룹 선택**)**를 선택합니다. 그룹을 추가하도록 선택하는 경우 새 그룹의 이름을 입력합니다. 디렉토리에서 선택하는 경우 필터 기준을 입력하고 **Retrieve Groups(**그룹 검색**)**를 클릭합니다. 선택할 그룹 옆의 확인란을 선택하고 **OK(**확인**)**를 클릭합니다. 선택한 그룹이 **Groups(**그룹**)** 창에 표시됩니다.

LDAP 속성 설정

표 *5: LDAP* 속성 설정

필드 이름	사용 지침
Add(추가**)**	새 속성을 추가하려면 **Add(**추가**) > Add Attribute(**속성 추가**)**를 선택합니다. 또는 LDAP 서버에서 속성을 선택하려면 **Add(**추가**) > Select Attributes From Directory(**디렉토리에서 속성 선택**)**를 선택합니다. 속성을 추가하도록 선택하는 경우 새 속성의 이름을 입력합니다. 디렉토리에서 선택하는 경우 사용자 이름을 입력하고 **Retrieve Attributes(**속성 검색**)**를 클릭하여 속성을 검색합니다. 선택할 속성 옆의 확인란을 선택하고 OK(확인)를 클릭합니다.

LDAP 고급 설정

다음 표에서는 Advanced Settings(고급 설정) 탭의 필드에 대해 설명합니다.

표 *6: LDAP* 고급 설정

필드 이름	사용 지침
Enable Password Change(비밀번호 변경 활성화**)**	디바이스 관리자에 PAP 프로토콜을 사용하고 네트워크 액세스에 RADIUS EAP-GTC 프로토콜을 사용하는 동안 비밀번호 만료 또는 비밀번호 재설정이 발생할 때 사용자가 비밀번호를 변경할 수 있도록하려면 이 확인란을 선택합니다. 지원되지 않는 프로토콜에 대한 사용자 인증은 실패합니다. 또한 이 옵션을 사용하면 사용자가 다음 로그인 시 비밀번호를 변경할 수 있습니다.

관련 항목

LDAP 디렉토리 서비스, 138 페이지
LDAP 사용자 인증, 140 페이지
LDAP 사용자 조회, 143 페이지
LDAP ID 소스 추가, 143 페이지

RADIUS 토큰 ID 소스 설정

다음 표에서는 외부 RADIUS ID 소스를 구성하고 해당 소스에 연결하는 데 사용할 수 있는 RADIUS 토큰 ID 소스 창의 필드에 대해 설명합니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**) > Identity Management(ID** 관리**) > External Identity Sources(**외부 **ID** 소스**) > RADIUS Token(RADIUS** 토큰**)**입니다.

표 *7: RADIUS* 토큰 *ID* 소스 설정

필드 이름	사용 지침
Name(이름**)**	RADIUS 토큰 서버의 이름을 입력합니다. 최대 64자까지 입력할 수 있습니다.
Description(설명**)**	RADIUS 토큰 서버에 대한 설명을 입력합니다. 최대 문자 수는 1,024자입니다.
SafeWord Server(SafeWord 서버**)**	RADIUS ID 소스가 SafeWord 서버인 경우 이 확인란을 선택합니다.
Enable Secondary Server(보조 서버 활성화**)**	기본 서버에 오류가 발생하는 경우 백업으로 사용할 Cisco ISE용 보조 RADIUS 토큰 서버를 활성화하려면 이 확인란을 선택합니다. 이 확인란을 선택하는 경우 보조 RADIUS 토큰 서버를 구성해야 합니다.
Always Access Primary Server First(항상 기본 서버에 먼저 액세스**)**	Cisco ISE가 항상 기본 서버에 먼저 액세스하도록 하려면 이 옵션을 클릭합니다.
Fallback to Primary Server after(다음 시간 이후 기본 서버로 대체**)**	기본 서버에 연결할 수 없는 경우 Cisco ISE가 보조 RADIUS 토큰 서버를 사용하여 인증할 수 있는 시간(분)을 지정하려면 이 옵션을 클릭합니다. 이 시간이 경과하면 Cisco ISE는 기본 서버에 대한 인증을 재시도합니다.
기본 서버	
Host IP(호스트 **IP)**	기본 RADIUS 토큰 서버의 IP 주소를 입력합니다. 이 필드에는 문자열로 표시되는 유효한 IP 주소를 입력할 수 있습니다. 이 필드에 입력할 수 있는 문자는 숫자와 점(.)입니다.
Shared Secret(공유 암호**)**	이 연결에 대해 기본 RADIUS 토큰 서버에 구성된 공유 암호를 입력합니다.
Authentication Port(인증 포트**)**	기본 RADIUS 토큰 서버가 수신 대기 중인 포트 번호를 입력합니다.
Server Timeout(서버 시간 초과**)**	기본 RADIUS 토큰 서버가 다운되었다고 결정할 때까지 Cisco ISE가 기본 서버로부터의 응답을 대기할 시간을 초 단위로 지정합니다.
Connection Attempts(연결 시도 횟수**)**	Cisco ISE가 보조 서버(정의된 경우)로 이동하거나 보조 서버가 정의되어 있지 않은 경우 요청을 삭제하기 전에 기본 서버에 다시 연결을 시도해야 하는 횟수를 지정합니다.

필드 이름	사용 지침
보조 서버	
Host IP(호스트 **IP)**	보조 RADIUS 토큰 서버의 IP 주소를 입력합니다. 이 필드에는 문자열로 표시되는 유효한 IP 주소를 입력할 수 있습니다. 이 필드에 입력할 수 있는 문자는 숫자와 점(.)입니다.
Shared Secret(공유 암호**)**	이 연결에 대해 보조 RADIUS 토큰 서버에 구성된 공유 암호를 입력합니다.
Authentication Port(인증 포트**)**	보조 RADIUS 토큰 서버가 수신 대기 중인 포트 번호를 입력합니다. 유효한 값은 1~65,535입니다. 기본값은 1,812입니다.
Server Timeout(서버 시간 초과**)**	보조 RADIUS 토큰 서버가 다운되었다고 결정할 때까지 Cisco ISE가 보조 서버로부터의 응답을 대기할 시간을 초 단위로 지정합니다.
Connection Attempts(연결 시도 횟수**)**	Cisco ISE가 요청을 삭제하기 전에 보조 서버에 다시 연결을 시도해야 하는 횟수를 지정합니다.

관련 항목

RADIUS 토큰 ID 소스, 163 페이지
RADIUS 토큰 서버 추가, 169 페이지

RSA SecurID ID 소스 설정

다음 표에서는 RSA SecurID ID 소스를 생성하고 해당 소스에 연결하는 데 사용할 수 있는 RSA SecurID ID 소스 페이지의 필드에 대해 설명합니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **External Identity Sources(**외부 **ID** 소스**)** > **RSA SecurID**입니다.

RSA 프롬프트 설정

다음 표에서는 **RSA Prompts(RSA** 프롬프트**)** 탭의 필드에 대해 설명합니다.

표 ***8: RSA*** 프롬프트 설정

필드 이름	사용 지침
Enter Passcode Prompt(암호 프롬프트 입력**)**	암호를 가져오기 위한 텍스트 문자열을 입력합니다.
Enter Next Token Code(다음 토큰 코드 입력**)**	다음 토큰을 요청하기 위한 텍스트 문자열을 입력합니다.

필드 이름	사용 지침
Choose PIN Type(PIN 유형 선택**)**	PIN 유형을 요청하기 위한 텍스트 문자열을 입력합니다.
Accept System PIN(시스템 **PIN** 수락**)**	시스템에서 생성된 핀 번호를 수락하기 위한 텍스트 문자열을 입력합니다.
Enter Alphanumeric PIN(영숫자 **PIN** 입력**)**	영숫자 PIN을 요청하기 위한 텍스트 문자열을 입력합니다.
Enter Numeric PIN(숫자 **PIN** 입력**)**	숫자 PIN을 요청하기 위한 텍스트 문자열을 입력합니다.
Re-enter PIN(PIN 다시 입력**)**	사용자에게 PIN을 다시 입력하도록 요청하기 위한 텍스트 문자열을 입력합니다.

RSA 메시지 설정

다음 표에서는 **RSA Messages(RSA** 메시지**)** 탭의 필드에 대해 설명합니다.

표 ***9: RSA*** 메시지 설정

필드 이름	사용 지침
Display System PIN Message(시스템 **PIN** 메시지 표시**)**	시스템 PIN 메시지에 레이블을 지정하기 위한 텍스트 문자열을 입력합니다.
Display System PIN Reminder(시스템 **PIN** 알림 표시**)**	사용자에게 새 PIN을 저장하도록 알리기 위한 텍스트 문자열을 입력합니다.
Must Enter Numeric Error(숫자를 입력해야 함 오류**)**	사용자에게 PIN에 숫자만 입력해야 하도록 지시하기 위한 메시지를 입력합니다.
Must Enter Alpha Error(영숫자를 입력해야 함 오류**)**	사용자에게 PIN에 영숫자 문자만 입력해야 하도록 지시하기 위한 메시지를 입력합니다.
PIN Accepted Message(PIN 수락됨 메시지**)**	사용자의 PIN이 시스템에서 수락되면 표시되는 메시지를 입력합니다.
PIN Rejected Message(PIN 거부됨 메시지**)**	시스템에서 사용자의 PIN을 거부하면 표시되는 메시지를 입력합니다.
User Pins Differ Error(사용자 **PIN**이 다름 오류**)**	사용자가 잘못된 PIN을 입력하면 표시되는 메시지를 입력합니다.
System PIN Accepted Message(시스템이 **PIN**을 수락함 메시지**)**	시스템에서 PIN을 수락하면 사용자에게 표시되는 메시지를 입력합니다.

필드 이름	사용 지침
Bad Password Length Error(잘못된 비밀번호 길이 오류**)**	사용자가 지정한 PIN이 PIN 길이 정책에 지정된 범위를 벗어나면 표시되는 메시지를 입력합니다.

관련 항목

RSA ID 소스, 170 페이지
Cisco ISE와 RSA SecurID 서버 통합, 171 페이지
RSA ID 소스 추가, 174 페이지

Cisco ISE 사용자

이 장에서 사용자란 용어는 네트워크에 정기적으로 액세스하는 직원 및 계약자, 그리고 스폰서 및 게스트 사용자를 가리킵니다. 스폰서 사용자는 스폰서 포털을 통해 guest-user 계정을 생성하고 관리하는 조직의 직원 또는 계약자입니다. 게스트 사용자는 제한된 기간 동안 조직의 네트워크 리소스에 액세스해야 하는 외부 방문자입니다.

사용자가 Cisco ISE 네트워크의 리소스 및 서비스에 대한 액세스를 얻으려면 관리자가 계정을 생성해야 합니다. 직원, 계약자 및 스폰서 사용자는 관리 포털에서 생성합니다.

사용자 ID

사용자 ID는 사용자에 대한 정보를 보유하는 컨테이너와 유사하며 네트워크 액세스 자격 증명을 형성합니다. 각 사용자의 ID는 데이터로 정의되며 사용자 이름, 이메일 주소, 비밀번호, 계정 설명, 연결된 관리 그룹, 사용자 그룹 및 역할을 포함합니다.

사용자 그룹

사용자 그룹은 특정 Cisco ISE 서비스 및 기능 집합에 액세스할 수 있게 해주는 공통 권한 집합을 공유하는 개인 사용자 컬렉션입니다.

사용자 ID 그룹

사용자의 그룹 ID는 동일 그룹에 속하는 특정 사용자 그룹을 식별하고 설명하는 요소로 이루어집니다. 그룹 이름은 이 그룹의 멤버가 지닌 기능적 역할에 대한 설명입니다. 그룹은 이 그룹에 속하는 사용자 목록입니다.

기본 사용자 ID 그룹

Cisco ISE에서는 다음과 같이 미리 정의된 사용자 ID 그룹이 제공됩니다.

- All_Accounts
- 직원

- Group_Accounts
- GuestType_Contractor
- GuestType_Daily
- GuestType_SocialLogin
- GuestType_Weekly
- Own_Accounts

사용자 역할

사용자 역할은 사용자가 수행할 수 있는 작업 및 Cisco ISE 네트워크에서 액세스할 수 있는 서비스를 결정하는 권한 집합입니다. 사용자 역할은 사용자 그룹과 연결됩니다(예: 네트워크 액세스 사용자).

사용자 계정 맞춤형 속성

Cisco ISE를 통해 네트워크 액세스 사용자와 관리자 모두의 사용자 속성에 따라 네트워크 액세스를 제한할 수 있습니다. Cisco ISE에서는 미리 정의된 사용자 속성 집합이 제공되며 이를 통해 사용자 맞춤화 속성을 생성할 수도 있습니다. 두 속성 유형을 모두 인증 정책을 정의하는 조건에 사용할 수 있습니다. 또한 비밀번호가 지정된 기준을 충족하도록 사용자 계정에 대한 비밀번호 정책을 정의할 수 있습니다.

사용자 맞춤화 사용자 속성

User Custom Attributes(사용자 맞춤화 속성**)** 창(**Administration(**관리**) > Identity Management(ID** 관리**) > Settings(**설정**) > User Custom Attributes(**사용자 맞춤화 속성**)**)에서 user-account 속성을 추가로 구성할 수 있습니다. 이 창에서 미리 정의된 사용자 속성 목록을 볼 수도 있습니다. 미리 정의된 사용자 속성은 수정할 수 없습니다.

User Custom Attributes(사용자 맞춤화 속성**)** 패널에 필요한 세부정보를 입력하여 새 맞춤화 속성을 추가합니다. **User Custom Attributes(**사용자 맞춤화 속성**)** 창에 추가한 맞춤화 속성 및 기본값이 네트워크 액세스 사용자(**Administration(**관리**) > Identity Management(ID** 관리**) > Identities(ID) > Users(**사용자**) > Add/Edit(**추가/편집**)**) 또는 관리 사용자(**Administration(**관리**) > System(**시스템**) > Admin Access(**관리자 액세스**) > Administrators(**관리자**) > Admin Users(**관리 사용자**) > Add/Edit(**추가/편집**)**)를 추가하거나 편집하는 동안 표시됩니다. 네트워크 액세스 또는 관리 사용자를 추가하거나 편집하는 동안 기본값을 변경할 수 있습니다.

User Custom Attributes(사용자 맞춤화 속성**)** 창에서 사용자 맞춤화 속성에 대해 다음 데이터 유형을 선택할 수 있습니다.

- 문자열: 최대 문자열 길이(문자열 속성 값에 허용되는 최대 길이)를 지정할 수 있습니다.
- 정수: 최솟값과 최댓값을 구성할 수 있습니다(허용되는 최저 및 최고 정수 값 지정).
- 열거형: 각 매개변수에 대해 다음 값을 지정할 수 있습니다.
    - 정수 값

- 표시 값

기본 매개변수를 지정할 수도 있습니다. 네트워크 액세스 또는 관리 사용자를 추가하거나 편집하는 동안 Display(표시) 필드에 추가한 값이 표시됩니다.

- 부동 소수점
- 비밀번호: 최대 문자열 길이를 지정할 수 있습니다.
- 길이: 최솟값과 최댓값을 구성할 수 있습니다.
- IP: 기본 IPv4 또는 IPv6 주소를 지정할 수 있습니다.
- 부울: True 또는 False를 기본값으로 설정할 수 있습니다.
- 날짜: 일정표에서 날짜를 선택하여 기본값으로 설정할 수 있습니다. 날짜는 yyyy-mm-dd 형식으로 표시됩니다.

네트워크 액세스 또는 관리 사용자를 추가하거나 편집하는 동안 속성을 필수로 지정하려면 **Mandatory(**필수**)** 확인란을 선택합니다. 사용자 맞춤화 속성에 대한 기본값을 설정할 수도 있습니다.

사용자 맞춤화 속성은 인증 정책에서도 사용 가능합니다. 사용자 맞춤화 속성에 대해 설정한 데이터 유형 및 허용 범위는 정책 조건의 사용자 맞춤화 속성 값에 적용됩니다.

사용자 인증 설정

일부 외부 ID 저장소에서는 네트워크 액세스 사용자가 비밀번호를 변경할 수 없습니다. 자세한 내용은 각 ID 소스에 대한 섹션을 참조하십시오.

네트워크 사용 비밀번호 규칙은 **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **Settings(**설정**)** > **User Authentication Settings(**사용자 인증 설정**)**에 구성됩니다.

다음 섹션에는 **Password Policy(**비밀번호 정책**)** 탭의 일부 필드에 대한 추가 정보가 있습니다.

- **Required characters(**필수 문자**)**: 대문자나 소문자가 필요한 사용자 비밀번호 정책을 구성했는데 사용자의 언어가 이러한 문자를 지원하지 않는 경우 사용자는 비밀번호를 설정할 수 없습니다. UTF-8 문자를 지원하려면 다음 확인란의 선택을 취소하십시오.
  - 소문자 알파벳 문자
  - 대문자 알파벳 문자
- **Password Change Delta(**비밀번호 변경 델타**)**: 현재 비밀번호를 새 비밀번호로 변경할 때 수정해야 하는 최소 문자 수를 지정합니다. Cisco ISE에서는 문자 위치 변경을 수정으로 간주하지 않습니다.

  예를 들어 비밀번호 델타가 3이고 현재 비밀번호가 "?Aa1234?"인 경우 "?Aa1567?" (3개의 새 문자는 "5","6" 및 "7")이 유효한 새 비밀번호입니다. "?Aa1562?"는 현재 비밀번호에 사용된 "?","2" 및 "?"가 있으므로 설정할 수 없습니다. "Aa1234??" 역시 사용할 수 없는데, 문자 위치가 변경되었더라도 동일한 문자가 현재 비밀번호에 있기 때문입니다.

비밀번호 변경 델타도 이전 X 비밀번호를 고려합니다. 여기서 X는 비밀번호는 이전 버전과 달라야 함의 값입니다. 비밀번호 델타가 3이고 비밀번호 기록이 2라면 과거 2개의 비밀번호에 포함되지 않은 문자 4개를 변경해야 합니다.

- **Dictionary words(**사전 단어**)**: 사전 단어의 사용, 역순으로 된 문자 또는 다른 문자로 대체되는 문자를 제한하려면 이 확인란을 선택합니다.

  "s"를 "$", "a"를 "@", "o"를 "0", "l"을 "1", "i"를 "!", "e"를 "3"으로 대체할 수 없습니다. 예를 들면 "Pa$$w0rd"입니다.

  - **Default Dictionary(**기본 사전**)**: Cisco ISE에서 기본 Linux 사전을 사용하려면 이 옵션을 선택합니다. 기본 사전에는 약 480,000개의 영어 단어가 포함되어 있습니다.
  - **Custom Dictionary(**맞춤형 사전**)**: 맞춤 설정한 사전을 사용하려면 이 옵션을 선택합니다. **Choose File(**파일 선택**)**을 클릭하여 맞춤형 사전 파일을 선택합니다. 텍스트 파일은 새 줄 구분된 단어, .dic 확장자여야 하며 크기가 20MB 미만이어야 합니다.

- **Password Lifetime(**비밀번호 수명**)** 섹션을 사용하여 비밀번호 재설정 간격 및 알림을 업데이트할 수 있습니다. 비밀번호 수명을 설정하려면 **Disable user account after __ days if password was not changed(**비밀번호를 변경하지 않으면 __일 후 사용자 계정 비활성화**)** 확인란을 선택하고 입력 필드에 일 수를 입력합니다. 비밀번호 재설정을 위해 미리 알림 이메일을 전송하려면 **Display Reminder __ Days Before Password Expiration(**비밀번호 만료 전 __ 일 이전 비밀번호 표시**)** 확인란을 선택하고 네트워크 액세스 사용자에 대해 구성된 이메일 주소로 미리 알림 이메일을 전송해야 하는 기간(일)을 입력합니다. 네트워크 액세스 사용자를 생성하는 동안 **Administration(**관리**) > Identity Management(ID** 관리**) > Identities(ID) > Users(**사용자**) > Add Network Access User(**네트워크 액세스 사용자 추가**)** 창에서 이메일 주소를 추가하여 비밀번호 재설정을 위한 이메일 알림을 보낼 수 있습니다.

  참고

  - 다음 이메일 주소에서 미리 알림 이메일이 전송됩니다. iseadminportal@<ISE-Primary-FQDN>. 이 발신자에 대한 액세스를 명시적으로 허용해야 합니다.
  - 이메일 내용은 사용자 지정할 수 없습니다. 알림 이메일의 내용은 다음과 같습니다. 네트워크 액세스 비밀번호는 <비밀번호 만료 날짜 및 시간>에 만료됩니다. 도움이 필요한 경우 시스템 관리자에게 문의하십시오.

- **Lock/Suspend Account with Incorrect Login Attempts(**잘못된 로그인 시도 시 계정 잠금/일시 중지**)**: 로그인 시도가 지정된 횟수만큼 실패한 경우 이 옵션을 사용하여 계정을 일시 중지하거나 잠글 수 있습니다. 유효 범위는 3~20입니다.

- **Account Disable Policy(**계정 비활성화 정책**)** 탭에서는 기존 사용자 계정을 비활성화할 시기에 대한 규칙을 구성합니다. 자세한 내용은 전역적으로 사용자 계정 비활성화를 참조하십시오.

관련 항목

사용자 계정 맞춤형 속성, 20 페이지

사용자 추가, 23 페이지

사용자 및 관리자의 자동 비밀번호 생성

사용자 및 관리자 생성 창에서는 Cisco ISE 비밀번호 정책을 준수하는 인스턴트 비밀번호를 생성하는 **Generate Password(**비밀번호 생성**)** 옵션을 사용할 수 있습니다. 따라서 사용자나 관리자는 구성할 안전한 비밀번호를 생각하는 데 시간을 소비하는 대신 Cisco ISE에서 생성하는 비밀번호를 사용할 수 있습니다.

Generate Password(비밀번호 생성**)** 옵션은 다음 창에서 사용할 수 있습니다.

- **Administration(**관리**) > Identity Management(ID** 관리**) > Identities(ID) > Users(**사용자**)**
- **Administration(**관리**) > System(**시스템**) > Admin Access(**관리자 액세스**) > Administrators(**관리자**) > Admin Users(**관리자 사용자**)**.
- **Settings(**설정**) > Account Settings(**계정 설정**) > Change Password(**비밀번호 변경**)**.

내부 사용자 작업

사용자 추가

Cisco ISE에서는 Cisco ISE 사용자의 속성에 대해 확인/생성/수정/복제/삭제/상태 변경/가져오기/내보내기/검색을 수행할 수 있습니다.

Cisco ISE 내부 데이터베이스를 사용 중인 경우에는 Cisco ISE 네트워크의 리소스나 서비스에 액세스해야 하는 새 사용자에 대해 계정을 생성해야 합니다.

단계 **1** **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **Identities(ID)** > **Users(**사용자**)**를 선택합니다.

Work Centers(작업 센터**)** > **Device Administration(**디바이스 관리**)** > **Identities(ID)** > **Users(**사용자**)** 페이지에 액세스하여 사용자를 생성할 수도 있습니다.

단계 **2** 새 사용자를 생성하려면 **Add (+)(**추가**(+))**를 클릭합니다.

단계 **3** 필드에 값을 입력합니다**.**

사용자 이름에 !, %, :, ;, [, {, |, },], `, ?, =, <, >, \ 문자와 제어 문자를 포함하지 마십시오. 공백으로만 구성된 사용자 이름도 허용되지 않습니다. BYOD용으로 Cisco ISE 내부 CA(Certificate Authority)를 사용하는 경우 여기에 입력하는 사용자 이름이 엔드포인트 인증서의 공용 이름으로 사용됩니다. Cisco ISE 내부 CA는 Common Name(공용 이름) 필드에서 "+" 또는 "*" 문자를 지원하지 않습니다.

단계 **4** 새 사용자를 Cisco ISE 내부 데이터베이스에 저장하려면 **Submit(**제출**)**을 클릭합니다.

Cisco ISE 사용자 데이터 내보내기

Cisco ISE 내부 데이터베이스에서 사용자 데이터를 내보내야 할 수 있습니다. Cisco ISE에서는 비밀번호로 보호된 csv 파일 형식으로 사용자 데이터를 내보낼 수 있습니다.

단계 **1** **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **Identities(ID)** > **Users(**사용자**)**를 선택합니다.

단계 **2** 데이터를 내보낼 사용자에 해당하는 확인란을 선택합니다.

단계 **3** **Export Selected(**선택 항목 내보내기**)**를 클릭합니다.

단계 **4** Key(키) 필드에 비밀번호를 암호화하는 키를 입력합니다.

단계 **5** users.csv 파일을 생성하려면 **Start Export(**내보내기 시작**)**를 클릭합니다.

단계 **6** users.csv 파일을 내보내려면 **OK(**확인**)**를 클릭합니다.

Cisco ISE 내부 사용자 가져오기

CSV 파일을 사용하여 새 사용자 데이터를 ICisco SE로 가져와 내부 계정을 새로 생성할 수 있습니다. 사용자 계정을 가져오는 동안 템플릿 CSV 파일 다운로드가 가능합니다. 스폰서는 스폰서 포털에서 사용자를 가져올 수 있습니다. 를 참조하십시오.

참고 CSV 파일에 맞춤형 속성이 포함되어 있으면 가져오는 동안 맞춤형 속성에 대해 설정한 데이터 유형 및 허용 범위가 맞춤형 속성 값에 적용됩니다.

단계 **1** **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **Identities(ID)** > **Users(**사용자**)**를 선택합니다.

단계 **2** 쉼표로 구분된 텍스트 파일에서 사용자를 가져오려면 **Import(**가져오기**)**를 클릭합니다.

쉼표로 구분된 텍스트 파일이 없으면 **Generate a Template(**템플릿 생성**)**을 클릭하여 제목 행이 채워진 CSV 파일을 생성합니다.

단계 **3** File(파일) 텍스트 상자에 가져올 사용자가 포함된 파일명을 입력하거나 **Browse(**찾아보기**)**를 클릭하고 파일이 있는 위치로 이동합니다.

단계 **4** 새 사용자를 생성하는 동시에 기존 사용자를 업데이트하려면 **Create new user(s) and update existing user(s) with new data(**새 사용자를 생성하고 새 데이터로 기존 사용자 업데이트**)** 확인란을 선택합니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

참고 모든 네트워크 액세스 사용자를 한 번에 삭제하지 않는 것이 좋습니다. 한 번에 삭제하면 CPU 사용량이 급증하여 서비스가 충돌할 수 있습니다(특히 매우 큰 데이터베이스를 사용하는 경우).

엔드포인트 설정

다음 표에서는 엔드포인트를 생성하고 엔드포인트용 정책을 할당하는 데 사용할 수 있는 **Endpoints(**엔드포인트**)** 창의 필드에 대해 설명합니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Network Access(**네트워크 액세스**)** > **Identities(ID)** > **Endpoints(**엔드포인트**)**입니다.

표 ***10:*** 엔드포인트 설정

필드 이름	사용 지침
MAC Address(MAC 주소**)**	정적으로 엔드포인트를 생성하기 위한 MAC 주소를 16진수 형식으로 입력합니다. MAC 주소는 Cisco ISE가 활성화된 네트워크에 연결되어 있는 인터페이스의 디바이스 식별자입니다.
Static Assignment(정적 할당**)**	정적 할당 상태가 정적으로 설정되어 있을 때 엔드포인트 창에서 엔드포인트를 정적으로 생성하려면 이 확인란을 선택합니다. 엔드포인트의 정적 할당 상태는 정적에서 동적으로 또는 동적에서 정적으로 전환할 수 있습니다.
Policy Assignment(정책 할당**)**	(**Static Assignment(**정적 할당**)**가 선택되어 있지 않으면 기본적으로 비활성화됨) **Policy Assignment(**정책 할당**)** 드롭다운 목록에서 일치하는 엔드포인트 정책을 선택합니다. 다음 중 하나를 수행할 수 있습니다. • 일치하는 엔드포인트 정책을 선택하지 않고 기본 엔드포인트 정책인 Unknown(알 수 없음)을 사용하는 경우 엔드포인트의 동적 프로파일링을 허용하는 엔드포인트에 대해 정적 할당 상태가 동적으로 설정됩니다. • Unknown(알 수 없음) 이외의 일치하는 엔드포인트 정책을 선택하는 경우에는 해당 엔드포인트에 대해 정적 할당 상태가 정적으로 설정되며 **Static Assignment(**정적 할당**)** 확인란이 자동으로 선택됩니다.

필드 이름	사용 지침
Static Group Assignment(정적 그룹 할당**)**	엔드포인트를 ID 그룹에 정적으로 할당하려면 이 확인란을 선택합니다. 이 확인란을 선택하면 이전에 다른 엔드포인트 ID 그룹에 동적으로 할당되었던 엔드포인트에 대해 다음 번에 엔드포인트 정책을 평가하는 동안 프로파일링 서비스가 엔드포인트 ID 그룹을 변경하지 않습니다. 이 확인란의 선택을 취소하면 정책 컨피그레이션에 따라 엔드포인트 ID 그룹이 ISE 프로파일러가 할당한 대로 동적으로 설정됩니다. Static Group Assignment(정적 그룹 할당) 옵션을 선택하지 않으면 다음 번에 엔드포인트 정책을 평가하는 동안 엔드포인트가 일치하는 ID 그룹에 자동으로 할당됩니다.

Identity Group Assignment(ID 그룹 할당**)**	엔드포인트를 할당할 엔드포인트 ID 그룹을 선택합니다.
	
	엔드포인트에 대한 엔드포인트 정책 평가 중에 **Create Matching Identity Group(**일치하는 **ID** 그룹 생성**)** 옵션을 사용하지 않으려는 경우 또는 엔드포인트를 정적으로 생성하는 경우 ID 그룹에 엔드포인트를 할당할 수 있습니다.
	
	Cisco ISE에는 시스템에서 생성된 다음과 같은 엔드포인트 ID 그룹이 포함되어 있습니다.
	• Blocked List
	• GuestEndpoints
	• Profiled
	  • Cisco IP-Phone
	  • Workstation
	• RegisteredDevices
	• Unknown

관련 항목

식별된 엔드포인트, 251 페이지
정책 및 ID 그룹을 정적으로 할당하여 엔드포인트 생성, 246 페이지

LDAP에서 엔드포인트 가져오기 설정

다음 표에서는 LDAP 서버에서 엔드포인트를 가져오는 데 사용할 수 있는 Import from LDAP(LDAP에서 가져오기) 창의 필드에 대해 설명합니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Network Access(**네트워크 액세스**)** > **Identities(ID)** > **Endpoints(**엔드포인트**)**입니다.

표 ***11: LDAP***에서 엔드포인트 가져오기 설정

필드 이름	사용 지침
Connection Settings(연결 설정**)**	
Host(호스트**)**	LDAP 서버의 호스트 이름 또는 IP 주소를 입력합니다.
Port(포트**)**	LDAP 서버의 포트 번호를 입력합니다. LDAP 서버에서 가져오려는 경우 기본 포트인 389를 사용할 수 있으며, SSL을 통해 LDAP 서버에서 가져오려는 경우 기본 포트인 636을 사용할 수 있습니다. 참고 Cisco ISE는 구성된 모든 포트 번호를 지원합니다. 구성된 값은 LDAP 서버 연결 세부정보와 일치해야 합니다.
Enable Secure Connection(보안 연결 활성화**)**	SSL을 통해 LDAP 서버에서 가져오려면 **Enable Secure Connection(**보안 연결 활성화**)** 확인란을 선택합니다.
Root CA Certificate Name(루트 **CA** 인증서 이름**)**	신뢰할 수 있는 CA 인증서를 보려면 드롭다운 화살표를 클릭합니다. 루트 CA 인증서 이름은 LDAP 서버에 연결하는 데 필요한 신뢰할 수 있는 CA 인증서를 지칭합니다. Cisco ISE에서는 신뢰할 수 있는 CA 인증서를 추가(가져오기), 편집, 삭제 및 내보내기할 수 있습니다.
Anonymous Bind(익명 바인딩**)**	**Anonymous Bind(**익명 바인딩**)** 확인란을 활성화하거나 slapd.conf 구성 파일에서 LDAP 관리자 자격 증명을 입력해야 합니다.
Admin DN(관리자 **DN)**	slapd.conf 구성 파일에서 LDAP 관리자에 대해 구성된 DN(Distinguished Name)을 입력합니다. 관리자 DN 형식의 예제는 cn=Admin, dc=cisco.com, dc=com과 같습니다.
Password(비밀번호**)**	slapd.conf 구성 파일에서 LDAP 관리자에 대해 구성된 비밀번호를 입력합니다.

필드 이름	사용 지침
Base DN(기본 **DN)**	부모 엔트리의 고유 이름을 입력합니다. 기본 DN 형식의 예제는 dc=cisco.com, dc=com과 같습니다.
Query Settings(쿼리 설정**)**	
MAC Address objectClass(MAC 주소 **objectClass)**	MAC 주소를 가져오는 데 사용되는 쿼리 필터(예: ieee802Device)를 입력합니다.
MAC Address Attribute Name(MAC 주소 속성 이름**)**	가져오려는 반환된 속성 이름(예: macAddress)을 입력합니다.
Profile Attribute Name(프로파일 속성 이름**)**	LDAP 속성의 이름을 입력합니다. 이 속성은 LDAP 서버에 정의되어 있는 각 엔드포인트 엔트리에 대한 정책 이름을 포함합니다. **Profile Attribute Name(**프로파일 속성 이름**)** 필드를 구성할 때는 다음 사항을 고려합니다. • **Profile Attribute Name(**프로파일 속성 이름**)** 필드에서 이 LDAP 속성을 지정하지 않거나 이를 잘못 구성하는 경우에는 가져오기 작업 중에 엔드포인트가 "알 수 없음"으로 표시되며 이러한 엔드포인트는 일치하는 엔드포인트 프로파일링 정책으로 별도로 프로파일이 지정됩니다. • **Profile Attribute Name(**프로파일 속성 이름**)** 필드에서 이 LDAP 속성을 구성하면 속성 값을 검증하여 엔드포인트 정책이 Cisco ISE의 기존 정책과 일치하는지를 확인한 다음, 엔드포인트를 가져옵니다. 엔드포인트 정책이 기존 정책과 일치하지 않으면 해당 엔드포인트를 가져오지 않습니다.
Time Out(시간 초과**)**	시간을 초 단위로 입력합니다. 유효한 범위는 1초 ~ 60초입니다.

관련 항목

식별된 엔드포인트, 251 페이지
LDAP 서버에서 엔드포인트 가져오기, 250 페이지

ID 그룹 작업

사용자 ID 그룹 생성

사용자 ID 그룹을 생성해야 해당 그룹에 사용자를 할당할 수 있습니다.

단계 1 **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **Groups(**그룹**)** > **Identity Groups(ID** 그룹**)** > **User Identity Groups(**사용자 **ID** 그룹**)** > **Add(**추가**)**를 선택합니다.

Work Centers(작업 센터**)** > **Device Administration(**디바이스 관리**)** > **User Identity Groups(**사용자 **ID** 그룹**)** > **Identity Groups(ID** 그룹**)** > **User Identity Groups(**사용자 **ID** 그룹**)** > **Add(**추가**)** 페이지에 액세스하여 사용자 ID 그룹을 생성할 수도 있습니다.

단계 2 Name(이름) 및 Description(설명) 필드에 값을 입력합니다. Name(이름) 필드에 입력할 수 있는 문자는 공백, # $ & ' ( ) * + - . / @ _입니다.

단계 3 **Submit(**제출**)**을 클릭합니다.

관련 항목

사용자 ID 그룹, 19 페이지

사용자 ID 그룹 내보내기

Cisco ISE에서는 로컬에 구성된 사용자 ID 그룹을 csv 파일 형식으로 내보낼 수 있습니다.

단계 1 **Administration(**관리**) > Identity Management(ID** 관리**) > Groups(**그룹**) > Identity Groups(ID** 그룹**) > User Identity Groups(**사용자 **ID** 그룹**)**를 선택합니다.

단계 2 내보낼 사용자 ID 그룹에 해당하는 확인란을 선택하고 **Export(**내보내기**)**를 클릭합니다.

단계 3 **OK(**확인**)**를 클릭합니다.

사용자 ID 그룹 가져오기

Cisco ISE에서는 사용자 ID 그룹을 csv 파일 형식으로 가져올 수 있습니다.

단계 1 **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **Groups(**그룹**)** > **Identity Groups(ID** 그룹**)** > **User Identity Groups(**사용자 **ID** 그룹**)**를 선택합니다.

단계 2 가져오기 파일에 사용할 템플릿을 가져오려면 **Generate a Template(**템플릿 생성**)**을 클릭합니다.

단계 3 쉼표로 구분된 텍스트 파일에서 네트워크 액세스 사용자를 가져오려면 Import(가져오기)를 클릭합니다.

단계 4 새 사용자 ID 그룹을 추가하는 동시에 기존 사용자 ID 그룹을 업데이트하려면 **Overwrite existing data with new data(**새 데이터로 기존 데이터 덮어쓰기**)** 확인란을 선택합니다.

단계 5 **Import(**가져오기**)**를 클릭합니다.

단계 6 변경사항을 Cisco ISE 데이터베이스에 저장하려면 **Save(**저장**)**를 클릭합니다.

엔드포인트 ID 그룹 설정

다음 표에서는 엔드포인트 그룹을 생성하는 데 사용할 수 있는 Endpoint Identity Groups(엔드포인트 ID 그룹) 창의 필드에 대해 설명합니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**) > Identity Management(ID** 관리**) > Groups(**그룹**) > Endpoint Identity Groups(**엔드포인트 **ID** 그룹**)**입니다.

표 *12:* 엔드포인트 *ID* 그룹 설정

필드 이름	사용 지침
Name(이름**)**	생성할 엔드포인트 ID 그룹의 이름을 입력합니다.
Description(설명**)**	생성할 엔드포인트 ID 그룹에 대한 설명을 입력합니다.
Parent Group(부모 그룹**)**	새로 생성하는 엔드포인트 ID 그룹을 연결할 엔드포인트 ID 그룹을 **Parent Group(**부모 그룹**)** 드롭다운 목록에서 선택합니다.

관련 항목

엔드포인트 ID 그룹에서 그룹화되어 식별된 엔드포인트, 253 페이지
엔드포인트 ID 그룹 생성, 253 페이지

최대 동시 세션 수 구성

최적의 성능을 위해 동시 사용자 세션 수를 제한할 수 있습니다. 사용자 레벨 또는 그룹 레벨에서 제한을 설정할 수 있습니다. 최대 사용자 세션 구성에 따라 세션 수가 사용자에게 적용됩니다.

ISE 노드당 각 사용자의 최대 동시 세션 수를 구성할 수 있습니다. 이 제한을 초과하는 세션은 거부됩니다.

단계 1 **Administration(**관리**) > System(**시스템**) > Settings(**설정**) > Max Sessions(**최대 세션 수**) > User(**사용자**)**를 선택합니다.

단계 2 다음 중 하나를 수행합니다.

- **Maximum Sessions per User(**사용자당 최대 세션 수**)** 필드에 각 사용자에게 허용되는 최대 동시 세션 수를 입력합니다.

  또는

- 사용자가 무제한 세션을 사용하도록 하려면 **Unlimited Sessions(**무제한 세션**)** 확인란을 선택합니다. 이 옵션은 기본적으로 선택되어 있습니다.

단계 **3** **Save(**저장**)**를 클릭합니다.

최대 세션 수가 사용자 레벨과 그룹 레벨에서 모두 구성된 경우 더 작은 값이 우선합니다. 예를 들어 사용자의 최대 세션 값이 10으로 설정되어 있고 사용자가 속한 그룹의 최대 세션 값이 5로 설정된 경우 사용자는 최대 5개의 세션만 사용할 수 있습니다.

그룹의 최대 동시 세션 수

ID 그룹의 최대 동시 세션 수를 구성할 수 있습니다.

때때로 그룹의 일부 사용자가 모든 세션을 사용하고 있을 수 있습니다. 이 경우 세션 수가 이미 구성된 최대 값에 도달했으므로 다른 사용자의 새 세션 생성 요청이 거부됩니다. Cisco ISE에서는 그룹에 있는 각 사용자의 최대 세션 제한을 구성할 수 있습니다. 특정 ID 그룹에 속한 각 사용자는 동일한 그룹의 다른 사용자가 연 세션 수에 관계없이 세션 제한보다 많은 세션을 열 수 없습니다. 특정 사용자의 세션 제한을 계산할 때 사용자당 전역 세션 제한, 사용자가 속한 ID 그룹당 세션 제한, 그룹의 사용자당 세션 제한 중 가장 낮은 구성 값이 우선합니다.

ID 그룹의 최대 동시 세션 수를 구성하려면 다음을 수행하십시오.

단계 **1** **Administration(**관리**) > System(**시스템**) > Settings(**설정**) > Max Sessions(**최대 세션 수**) > Group(**그룹**)**을 선택합니다.

구성된 모든 ID 그룹이 나열됩니다.

단계 **2** 편집할 그룹 옆에있는 Edit(편집) 아이콘을 클릭하고 다음 값을 입력합니다.

- 해당 그룹에 허용되는 최대 동시 세션 수. 그룹의 최대 세션 수가 100으로 설정된 경우, 해당 그룹의 모든 멤버가 설정한 모든 세션의 총 개수는 100개를 초과할 수 없습니다.

  참고 그룹 레벨 세션 제한은 그룹 계층 구조에 따라 적용됩니다.

- 해당 그룹의 각 사용자에 허용되는 최대 동시 세션 수. 이 옵션은 그룹의 최대 세션 수를 재정의합니다.

그룹의 최대 동시 세션 수 또는 그룹 내 사용자의 최대 동시 세션 수를 Unlimited(무제한)로 설정하려면 **Max Sessions for Group/Max Sessions for User for Group(**그룹의 최대 세션 수/그룹 내 사용자의 최대 세션 수**)** 필드를 비워두고 체크 표시 아이콘을 클릭한 다음 Save(저장)를 클릭합니다. 기본적으로 이 두 값은 모두 Unlimited(무제한)로 설정됩니다.

단계 **3** **Save(**저장**)**를 클릭합니다.

카운터 시간 제한 구성

동시 사용자 세션에 대한 시간 초과 값을 구성할 수 있습니다.

단계 **1** **Administration(**관리**) > System(**시스템**) > Settings(**설정**) > Max Sessions(**최대 세션 수**) > Counter Time Limit(**카운터 시간 제한**)**를 선택합니다.

단계 **2** 다음 옵션 중 하나를 선택합니다.

- **Unlimited(**무제한**)**: 세션의 시간 초과 또는 시간 제한을 설정하지 않으려면 이 확인란을 선택합니다.
- **Delete sessions after(**다음 시간 초과 후 세션 삭제**)**: 동시 세션의 시간 초과 값을 분, 시간 또는 일 단위로 입력할 수 있습니다. 세션이 시간 제한을 초과하면 Cisco ISE는 카운터에서 세션을 삭제하고 세션 수를 업데이트하여 새 세션을 허용합니다. 세션이 시간 제한을 초과해도 사용자는 로그아웃되지 않습니다.

단계 **3** **Save(**저장**)**를 클릭합니다.

RADIUS Live Logs(RADIUS 라이브 로그) 창에서 세션 수를 재설정할 수 있습니다. Identity(ID), Identity Group(ID 그룹) 또는 Server(서버) 열에 표시된 Actions(작업) 아이콘을 클릭하여 세션 수를 재설정합니다. 세션을 재설정하면 카운터에서 세션이 삭제됩니다(이에 따라 새 세션 사용 가능). 카운터에서 세션이 삭제되어도 사용자의 연결은 끊어지지 않습니다.

계정 비활성화 정책

Cisco ISE는 사용자 또는 관리자를 인증하거나 쿼리하는 동안 **Administration(**관리**) > Identity Management(ID** 관리**) > Settings(**설정**) > User Authentication Settings(**사용자 인증 설정**)** 창에서 전역 계정 비활성화 정책 설정을 확인한 다음 컨피그레이션에 따라 결과를 인증하거나 반환합니다.

Cisco ISE는 다음의 3가지 정책을 확인합니다.

- 지정된 날짜(yyyy-mm-dd)를 초과하는 사용자 계정 비활성화: 지정된 날짜에 사용자 계정을 비활성화합니다. 그러나 **Administration(**관리**) > Identity Management(ID** 관리**) > Identities(ID) > Users(**사용자**) > Account Disable Policy(**계정 비활성화 정책**)**에 구성되어 있는 개별 네트워크 액세스 사용자에 대한 계정 비활성화 정책 설정이 전역 설정보다 우선적으로 적용됩니다.
- Disable user account after *n* days of account created or last enable(계정 생성 후 또는 마지막 활성화 후 n일 시점에 사용자 비활성화): 계정 생성 이후 또는 계정이 활성 상태였던 마지막 날짜 이후 특정 기간(일)이 지나면 사용자 계정을 비활성화합니다. **Administration(**관리**) > Identity Management(ID** 관리**) > Identities(ID) > Users(**사용자**) > Status(**상태**)**에서 사용자 상태를 확인할 수 있습니다.
- Disable accounts after n days of inactivity(*n*일 동안 비활성 상태 후 계정 비활성화): 구성된 연속 기간(일) 동안 인증되지 않은 관리자 및 사용자 계정을 비활성화합니다.

Cisco Secure ACS에서 Cisco ISE로 마이그레이션할 때, Cisco Secure ACS에서 네트워크 액세스 사용자에 대해 지정된 계정 비활성화 정책 설정은 Cisco ISE로 마이그레이션됩니다.

개별 사용자 계정 비활성화

Cisco ISE에서는 관리 사용자가 지정한 날짜가 사용자 레벨에서 초과되는 경우 각 개별 사용자의 사용자 계정을 비활성화할 수 있습니다.

단계 **1** **Administration(**관리**) > Identity Management(ID** 관리**) > Identities(ID)> Users(**사용자**)**를 선택합니다.

단계 **2** **Add(**추가**)**를 클릭하여 새 사용자를 생성하거나 기존 사용자 옆에 있는 확인란을 선택하고 **Edit(**편집**)**를 클릭하여 기존 사용자 세부정보를 편집합니다.

단계 **3** **Disable account if the date exceeds(**날짜가 초과되는 경우 계정 비활성화**)** 확인란을 선택하고 날짜를 선택합니다.

이 옵션을 사용하면 구성된 날짜가 초과될 때 사용자 계정을 비활성화할 수 있습니다. 필요에 따라 서로 다른 사용자에 대해 서로 다른 만료 날짜를 구성할 수 있습니다. 이 옵션은 각 개별 사용자의 전역 컨피그레이션을 무효화합니다. 구성된 날짜는 현재 시스템 날짜일 수도 있고 이후의 날짜일 수도 있습니다.

참고 현재 시스템 날짜 이전의 날짜는 입력할 수 없습니다.

단계 **4** 개별 사용자에 대한 계정 비활성화 정책을 구성하려면 **Submit(**제출**)**을 클릭합니다.

전역적으로 사용자 계정 비활성화

특정 날짜, 계정 생성 또는 마지막 액세스 날짜 며칠 후, 계정이 비활성화되고 며칠 후 사용자 계정을 비활성화할 수 있습니다.

단계 **1** **Administration(**관리**) > Identity Management(ID** 관리**) > Settings(**설정**) > User Authentication Settings(**사용자 인증 설정**) > Account Disable Policy(**계정 비활성화 정책**)**를 선택합니다.

단계 **2** 다음 작업 중 하나를 수행합니다.

- **Disable account if date exceeds(**날짜가 초과되는 경우 계정 비활성화**)** 확인란을 선택하고 적절한 날짜를 yyyy-mm-dd 형식으로 선택합니다. 이 옵션을 사용하면 구성된 날짜가 지나고 사용자 계정을 비활성화할 수 있습니다. 사용자 레벨에서 **Disable account if date exceeds(**날짜가 초과되는 경우 계정 비활성화**)** 설정은 이 전역 컨피그레이션보다 우선합니다.
- **Disable account after n days of account creation or last enable(**계정 생성 또는 마지막 활성화 **n**일 후 계정 비활성화**)** 확인란을 선택하고 기간(일)을 입력합니다. 이 옵션을 사용하면 계정 생성 날짜 또는 마지막 액세스 날짜가 지정한 기간(일)을 초과하면 사용자 계정을 비활성화할 수 있습니다. 관리자는 비활성화된 사용자 계정을 수동으로 활성화할 수 있으며, 이후 일 수는 자동으로 재설정됩니다.
- **Disable account after n days of inactivity(n**일 동안 비활성 상태였던 계정 비활성화**)** 확인란을 선택하고 기간(일)을 입력합니다. 이 옵션을 사용하면 계정이 지정한 기간(일) 동안 비활성 상태일 때 사용자 계정이 비활성화됩니다.

단계 **3** 전역 계정 비활성화 정책을 구성하려면 **Submit(**제출**)**을 클릭합니다.

내부 및 외부 **ID** 소스

ID 소스는 사용자 정보를 저장하는 데이터베이스입니다. Cisco ISE는 ID 소스의 사용자 정보를 사용하여 인증 시 사용자 자격 증명을 검증합니다. 사용자 정보에는 그룹 정보 및 사용자와 연관된 기타 속성이 포함됩니다. ID 소스에서 사용자 정보를 추가 편집 및 삭제할 수 있습니다.

Cisco ISE는 내부 및 외부 ID 소스를 지원합니다. 두 소스를 모두 사용하여 스폰서 및 게스트 사용자를 인증할 수 있습니다.

내부 **ID** 소스

Cisco ISE에는 사용자 정보를 저장하는 데 사용할 수 있는 내부 사용자 데이터베이스가 있습니다. 내부 사용자 데이터베이스의 사용자는 내부 사용자라고 합니다. Cisco ISE에는 모든 디바이스 및 해당 디바이스에 연결되는 엔드포인트 관련 정보를 저장하는 내부 엔드포인트 데이터베이스도 있습니다.

외부 **ID** 소스

Cisco ISE에서는 사용자 정보가 포함된 외부 ID 소스를 구성할 수 있습니다. Cisco ISE는 인증을 위한 사용자 정보를 얻기 위해 외부 ID 소스에 연결합니다. 외부 ID 소스에는 Cisco ISE 서버 및 인증서 인증 프로파일의 인증서 정보도 포함됩니다. Cisco ISE는 외부 ID 소스와 통신하기 위해 인증 프로토콜을 사용합니다.

내부 사용자에 대한 정책을 구성할 때 다음 사항에 유의하십시오.

- 내부 ID 저장소에 대해 내부 사용자를 인증하도록 인증 정책을 구성합니다.
- 다음 옵션을 선택하여 내부 사용자 그룹에 대한 권한 부여 정책을 구성합니다.

  `Identitygroup.Name EQUALS User Identity Groups:` **`Group_Name`**

다음 표에는 인증 프로토콜과 해당 프로토콜에서 지원하는 외부 ID가 나와 있습니다.

표 ***13:*** 인증 프로토콜 및 지원되는 외부 ***ID*** 소스

프로토콜(인증 유형)	내부 데이터베이스	**Active Directory**	**LDAP**	**RADIUS** 토큰 서버 또는 **RSA**	**REST**	**ODBC**
EAP-GTC, PAP(일반 텍스트 비밀번호)	예	예	예	예	예	예
MS-CHAP 비밀번호 해시: MSCHAPv1/v2 EAP-MSCHAPv2(EAP, EAP-FAST, EAP-TTLS 또는 TEAP의 내부 방법) LEAP	예	예	아니요	아니요	아니요	예
EAP-MD5 CHAP	예	아니요	아니요	아니요	아니요	예

프로토콜(인증 유형)	내부 데이터베이스	Active Directory	LDAP	RADIUS 토큰 서버 또는 RSA	REST	ODBC
EAP-TLS PEAP-TLS (인증서 검색) 참고 TLS 인증(EAP-TLS 및 PEAP-TLS)에 ID 소스가 필요하지는 않지만 선택적으로 권한 부여 정책 조건에 대해 추가할 수 있습니다.	아니요	예	예	아니요	아니요	아니요

자격 증명은 외부 데이터 소스 연결 유형 및 사용된 기능에 따라 다르게 저장됩니다.

- Active Directory 도메인에 조인할 때(패시브 ID용이 아님) 조인하는 데 사용되는 자격 증명은 저장되지 않습니다. Cisco ISE는 AD 컴퓨터 계정이 없는 경우 이를 생성하고 해당 계정을 사용하여 사용자를 인증합니다.
- LDAP 및 패시브 ID의 경우 외부 데이터 소스에 연결하는 데 사용되는 자격 증명을 사용하여 사용자를 인증합니다.

외부 ID 소스 생성

Cisco ISE는 Active Directory LDAP, RADIUS 토큰 및 RSA SecurID 서버와 같은 외부 ID 소스에 연결하여 인증 및 권한 부여를 위한 사용자 정보를 가져올 수 있습니다. 외부 ID 소스에는 인증서 기반 인증에 필요한 인증서 인증 프로파일도 포함되어 있습니다.

참고 인증된 사용자 ID를 수신하고 공유할 수 있는 패시브 ID 서비스를 사용하려면 추가 패시브 ID 서비스 제공자, 94 페이지의 내용을 참조하십시오.

단계 1 Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(관리)** > **Identity Management(ID 관리)** > **External Identity Sources(외부 ID 소스)**를 선택합니다.

단계 2 다음 옵션 중 하나를 선택합니다.

- 인증서 기반 인증의 경우 **Certificate Authentication Profile(인증서 인증 프로파일)**을 선택합니다.
- 외부 ID 소스로 Active Directory에 연결하려는 경우 **Active Directory**를 선택합니다. 자세한 내용은 외부 ID 소스로서의 Active Directory, 38 페이지를 참조하십시오.
- LDAP ID 소스를 추가하려는 경우 **LDAP**를 선택합니다. 자세한 내용은 LDAP, 138 페이지를 참조하십시오.
- RADIUS 토큰 서버를 추가하려는 경우 **RADIUS** 토큰을 선택합니다. 자세한 내용은 RADIUS 토큰 ID 소스, 163 페이지를 참조하십시오.
- RSA SecurID 서버를 추가하려는 경우 **RSA SecurID**를 선택합니다. 자세한 내용은 RSA ID 소스, 170 페이지를 참조하십시오.
- Oracle Access Manager 등의 IdP(Identity Provider)를 추가하려는 경우 **SAML Id Provider(SAML ID 제공자)**를 선택합니다. 자세한 내용은 외부 ID 소스로서의 SAMLv2 ID 제공자, 177 페이지를 참조하십시오.
- 소셜 로그인(예: Facebook 등)을 외부 ID 소스로 추가하려면 **Social Login(소셜 로그인)**을 선택합니다. 자세한 내용은 셀프 등록 게스트의 소셜 로그인을(를) 참조하십시오.

외부 ID 저장소 비밀번호에 대해 내부 사용자 인증

Cisco ISE에서는 외부 ID 저장소 비밀번호에 대해 내부 사용자를 인증할 수 있습니다. Cisco ISE는 **Administration(관리)** > **Identity Management(ID 관리)** > **Identities(ID)** > **Users(사용자)** 창에서 내부 사용자에 대해 비밀번호 ID 저장소를 선택하는 옵션을 제공합니다. 관리자는 **Users(사용자)** 창에서 사용자를 추가하거나 편집하는 동안 Cisco ISE 외부 ID 소스 목록에서 ID 저장소를 선택할 수 있습니다. 내부 사용자의 기본 비밀번호 ID 저장소는 내부 ID 저장소입니다. Cisco Secure ACS 사용자의 경우 Cisco Secure ACS에서 Cisco ISE로 마이그레이션하는 중과 마이그레이션한 후에 비밀번호 ID 저장소가 동일하게 유지됩니다.

Cisco ISE는 비밀번호 유형에 대해 다음과 같은 외부 ID 저장소를 지원합니다.

- Active Directory
- LDAP
- ODBC
- RADIUS 토큰 서버
- RSA SecurID 서버

참고 현재 설계에 따라 외부 ID 저장소에 대해 인증이 수행되면 권한 부여 정책에서 내부 사용자 ID 그룹 이름을 구성할 수 없습니다. 권한 부여에 내부 사용자 ID 그룹을 사용하려면 내부 사용자 ID 저장소에 대해 인증하도록 인증 정책을 구성해야 하며 사용자 컨피그레이션에서 내부 또는 외부의 비밀번호 유형을 선택해야 합니다.

인증서 인증 프로파일

각 프로파일에 대해 보안 주체 사용자 이름으로 사용해야 하는 인증서 필드와 인증서의 이진 비교를 사용할지 여부를 지정해야 합니다.

인증서 인증 프로파일 추가

EAP-TLS(Extensible Authentication Protocol-Transport Layer Security) 인증서 기반 인증 방법을 사용하려는 경우 인증서 인증 프로파일을 생성해야 합니다. Cisco ISE는 기존 사용자 이름 및 비밀번호 방법을 통해 인증을 수행하는 대신 클라이언트로부터 받은 인증서를 서버의 인증서와 비교하여 사용자의 신뢰성을 확인합니다.

시작하기 전에

다음 작업을 수행하려면 슈퍼 관리자 또는 시스템 관리자여야 합니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **External Identity Sources(**외부 **ID** 소스**)** > **Certificate Authentication Profile(**인증서 인증 프로파일**)** > **Add(**추가**)**를 선택합니다.

단계 **2** 인증서 인증 프로파일의 이름과 설명(선택 사항)을 입력합니다.

단계 **3** 드롭다운 목록에서 ID 저장소를 선택합니다.

기본 인증서 확인 시에는 ID 소스가 필요하지 않습니다. 인증서에 대해 이진 비교 확인을 수행하려면 ID 소스를 선택해야 합니다. ID 소스로 Active Directory를 선택하는 경우에는 주체 이름과 일반 이름 및 대체 주체 이름(모든 값)을 사용하여 사용자를 조회할 수 있습니다.

단계 **4** **Certificate Attribute(**인증서 속성**)** 또는 **Any Subject or Alternative Name Attributes in the Certificate(**인증서의 모든 주체 또는 대체 이름 속성**)**에서 ID 사용 여부를 선택합니다. 이 ID는 로그와 조회에서 사용됩니다.

Any Subject or Alternative Name Attributes in the Certificate(인증서의 모든 주체 또는 대체 이름 속성**)**를 선택하면 Active Directory UPN이 로그의 사용자 이름으로 사용되며 인증서의 모든 주체 이름 및 대체 이름을 사용하여 사용자를 조회합니다. 이 옵션은 Active Directory를 ID 소스로 선택하는 경우에만 사용할 수 있습니다.

단계 **5** **Match Client Certificate Against Certificate In Identity Store(ID** 저장소의 인증서와 클라이언트 인증서 일치 여부 확인**)**을 수행할 경우를 선택합니다. 인증서 일치 여부를 확인하려면 ID 소스(LDAP 또는 Active Directory)를 선택해야 합니다. Active Directory를 선택하는 경우 모호한 ID를 확인하기 위한 용도로만 인증서 일치 여부를 확인하도록 선택할 수 있습니다.

- **Never(**안 함**)**: 이 옵션을 선택하면 이진 비교를 수행하지 않습니다.
- **Only to resolve identity ambiguity(ID** 모호성만 해결**)**: 이 옵션을 선택하면 모호한 ID가 발견되는 경우에 한해 Active Directory의 계정에 대한 인증서와 클라이언트 인증서의 이진 비교를 수행합니다. 인증서의 ID 이름과 일치하는 Active Directory 계정이 여러 개 발견된 경우를 예로 들 수 있습니다.
- **Always perform binary comparison(**항상 이진 비교 수행**)**: 이 옵션을 선택하면 ID 저장소(Active Directory 또는 LDAP)의 계정에 대한 인증서와 클라이언트 인증서의 이진 비교를 항상 수행합니다.

단계 **6** **Submit(**제출**)**을 클릭하여 인증서 인증 프로파일을 추가하거나 변경사항을 저장합니다.

외부 ID 소스로서의 Active Directory

Cisco ISE는 사용자, 머신, 그룹 및 속성과 같은 리소스에 액세스하기 위한 외부 ID 소스로 Microsoft Active Directory를 사용합니다. Active Directory의 사용자 및 머신 인증을 통해 Active Directory에 나열된 사용자 및 디바이스에만 네트워크에서 액세스할 수 있습니다.

ISE 커뮤니티 리소스

AD 자격 증명을 사용하는 ISE 관리 포털 액세스 컨피그레이션 예

Active Directory에서 지원되는 인증 프로토콜 및 기능

Active Directory에서는 일부 프로토콜과 함께 Active Directory 사용자 비밀번호를 변경하여 사용자 및 머신 인증과 같은 기능을 지원합니다. 다음 표에는 Active Directory에서 지원되는 인증 프로토콜과 각 기능이 나와 있습니다.

표 ***14: Active Directory***에서 지원되는 인증 프로토콜

인증 프로토콜	기능
EAP-FAST 및 비밀번호 기반 PEAP(Protected Extensible Authentication Protocol)	사용자 및 머신 인증, 내부 MS-CHAPv2 및 EAP-GTC 방법과 함께 EAP-FAST 및 PEAP를 사용하여 비밀번호를 변경할 수 있는 기능 포함
PAP(Password Authentication Protocol)	사용자 및 머신 인증
MS-CHAPv1(Microsoft Challenge Handshake Authentication Protocol Version 1)	사용자 및 머신 인증
MS-CHAPv2(Microsoft Challenge Handshake Authentication Protocol Version 2)	사용자 및 머신 인증
EAP-GTC(Extensible Authentication Protocol-Generic Token Card)	사용자 및 머신 인증

인증 프로토콜	기능
EAP-TLS(Extensible Authentication Protocol-Transport Layer Security)	• 사용자 및 머신 인증 • 그룹 및 속성 검색 • 이진 인증서 비교
EAP-FAST-TLS(Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling-Transport Layer Security)	• 사용자 및 머신 인증 • 그룹 및 속성 검색 • 이진 인증서 비교
PEAP-TLS(Protected Extensible Authentication Protocol-Transport Layer Security)	• 사용자 및 머신 인증 • 그룹 및 속성 검색 • 이진 인증서 비교
LEAP(Lightweight Extensible Authentication Protocol)	사용자 인증

권한 부여 정책에 사용할 **Active Directory** 속성 및 그룹 검색

Cisco ISE는 Active Directory에서 권한 부여 정책 규칙에 사용할 사용자 또는 머신 속성 및 그룹을 검색합니다. 이러한 속성은 Cisco ISE 정책에 사용될 수 있으며 사용자 또는 머신의 권한 부여 수준을 결정합니다. 성공적인 인증이 이루어지고 나면 Cisco ISE는 사용자 및 머신 Active Directory 속성을 검색하고 인증과 관계없는 권한 부여를 위한 속성도 검색할 수 있습니다.

Cisco ISE는 외부 ID 저장소의 그룹을 사용하여 사용자 또는 컴퓨터에 권한을 할당(예: 사용자를 스폰서 그룹에 매핑하기 위해)할 수 있습니다. Active Directory에서 그룹 멤버십에 대한 다음 제한 사항에 유의해야 합니다.

- 정책 규칙 조건은 사용자 또는 컴퓨터의 기본 그룹, 사용자 또는 컴퓨터가 직접 멤버인 그룹 또는 간접(중첩된) 그룹 중 하나를 참조할 수 있습니다.
- 사용자 또는 컴퓨터의 계정 도메인 외부에 있는 도메인 로컬 그룹은 지원되지 않습니다.

참고 Active Directory 속성, msRadiusFramedIPAddress의 값을 IP 주소로 사용할 수 있습니다. 인증 프로파일에 이 IP 주소를 포함하여 NAS(Network Access Server)로 전송할 수 있습니다. msRADIUSFramedIPAddress 속성은 IPv4 주소만 지원합니다. 사용자 인증 시 사용자에 대해 가져오는 msRadiusFramedIPAddress 속성 값은 IP 주소 형식으로 변환됩니다.

속성 및 그룹은 가입 지점별로 검색되고 관리됩니다. 이는 권한 부여 정책에 사용(먼저 가입 지점을 선택한 다음 속성 선택)됩니다. 권한 부여의 경우 범위에 따라 속성 또는 그룹을 정의할 수 없지만 인증 정책에 범위를 사용할 수는 있습니다. 인증 정책에 범위를 사용하는 경우 사용자는 한 가입 지점

을 통해 인증되지만 속성 및/또는 그룹은 사용자의 계정 도메인에 대한 신뢰 경로를 가진 다른 가입 지점을 통해 인증될 수 있습니다. 인증 도메인을 사용하여 인증 도메인에서 범위가 하나인 두 가입 지점이 겹치는 문제가 발생하지 않도록 할 수 있습니다.

참고 다중 가입 포인트 컨피그레이션의 권한 부여 프로세스 중에 Cisco ISE는 특정 사용자가 발견될 때까지만 권한 부여 정책에 나열된 순서대로 가입 포인트를 검색합니다. 사용자가 발견되면 가입 포인트에서 사용자에게 할당된 속성 및 그룹을 사용해 권한 부여 정책을 평가합니다.

참고 사용 가능한 Active Directory 그룹의 최대 수에 대한 Microsoft의 제한을 참고해 주십시오. http://technet.microsoft.com/en-us/library/active-directory-maximum-limits-scalability(v=WS.10).aspx

규칙에 특수 문자(예: /, !, @, \, #, $, %, ^, &, *, (,), _, + 또는 ~)를 가진 Active Directory 그룹 이름이 포함되면 권한 부여 정책이 실패하게 됩니다.

관리자 사용자 이름에 $ 문자가 포함되어 있으면 Active Directory를 통한 관리자 로그인이 실패할 수 있습니다.

명시적 **UPN** 사용

Active Directory의 UPN(User-Principal-Name) 속성과 사용자 정보를 일치시킬 때 모호성을 줄이려면 명시적 UPN을 사용하도록 Active Directory를 구성해야 합니다. 두 사용자의 *sAMAccountName* 값이 동일한 경우 암시적 UPN을 사용하면 모호한 결과가 생성 될 수 있습니다.

Active Directory에서 명시적 UPN을 설정하려면 **Advanced Tuning(**고급 조정**)** 페이지를 열고 *REGISTRY.Services\lsass\Parameters\Providers\ActiveDirectory\UseExplicitUPN* 속성을 1로 설정합니다.

부울 속성 지원

Cisco ISE는 Active Directory 및 LDAP ID 저장소에서 부울 속성 검색을 지원합니다.

Active Directory 또는 LDAP에 대한 디렉토리 속성을 구성하는 동안 부울 속성을 구성할 수 있습니다. 이러한 속성은 Active Directory 또는 LDAP 인증 시 검색됩니다.

부울 속성은 정책 규칙 조건을 구성하는 데 사용할 수 있습니다.

부울 속성 값은 Active Directory 또는 LDAP 서버에서 문자열 유형으로 가져옵니다. Cisco ISE는 부울 속성에 대해 다음 값을 지원합니다.

부울 속성	지원되는 값
True(참)	t, T, true, TRUE, True, 1
거짓	f, F, false, FALSE, False, 0

참고 부울 속성에 대한 속성 대체는 지원되지 않습니다.

부울 속성(예: msTSAllowLogon)을 문자열 유형으로 구성하는 경우 Active Directory 또는 LDAP 서버 내 속성의 부울 값이 Cisco ISE의 문자열 속성에 대해 설정됩니다. 속성 유형을 부울로 변경하거나 수동으로 속성을 부울 유형으로 추가할 수 있습니다.

인증서 기반 인증을 위한 **Active Directory** 인증서 검색

Cisco ISE는 EAP-TLS 프로토콜을 사용하는 사용자 및 머신 인증을 위해 인증서 검색을 지원합니다. Active Directory의 사용자 또는 머신 기록는 이진 데이터 유형의 인증서 속성을 포함합니다. 이 인증서 속성에는 하나 이상의 인증서가 포함될 수 있습니다. Cisco ISE는 이 속성을 userCertificate로 식별하며 이 속성에 대해 다른 이름을 구성하는 것을 허용하지 않습니다. Cisco ISE는 이 인증서를 검색하여 이진 비교를 수행하는 데 사용합니다.

인증서 인증 프로파일에 따라 Active Directory에서 인증서를 검색하는 데 사용할 사용자를 조회하기 위해 사용자 이름(예: SAN(Subject Alternative Name) 또는 일반 이름)을 가져오는 필드가 결정됩니다. Cisco ISE가 인증서를 검색한 후에는 이 인증서와 클라이언트 인증서의 이진 비교를 수행합니다. 여러 인증서가 검색되면 Cisco ISE는 인증서를 비교하여 일치하는 항목을 확인합니다. 일치하는 인증서가 발견되면 사용자 또는 머신 인증이 통과됩니다.

Active Directory 사용자 인증 프로세스 플로우

사용자를 인증하거나 쿼리하는 경우 Cisco ISE는 다음을 확인합니다.

- MS-CHAP 및 PAP 인증에서는 사용자가 비활성화, 잠금 또는 만료되었거나 로그온 시간을 벗어났는지 확인하고 이러한 조건 중 어느 것이든 충족하는 경우 인증이 실패합니다.
- EAP-TLS 인증에서는 사용자가 비활성화 또는 잠금되었는지 확인하고 조건 중 어느 것이든 충족하는 경우 인증이 실패합니다.

Azure Active Directory를 사용하여 사용자를 인증하기 위한 리소스 소유자 비밀번호 인증서 플로우 구성

주의 Cisco ISE의 ROPC(Resource Owner Password Credentials) 플로우는 제어되는 도입 기능입니다. 이 기능은 프로덕션 환경에서 사용하기 전에 테스트 환경에서 철저하게 테스트하는 것이 좋습니다.

ROPC(Resource Owner Password Credentials)는 클라우드 기반 ID 제공자가 있는 네트워크에서 Cisco ISE가 권한 부여 및 인증을 수행할 수 있도록 하는 OAuth 2.0 권한 부여 유형입니다.

Cisco ISE는 ROPC 플로우를 사용하여 클라우드 기반 ID 소스로 사용자의 자격 증명을 검증합니다. ROPC 플로우는 일반 텍스트 인증 프로토콜을 지원합니다.

Cisco ISE는 현재 ROPC 플로우를 통해 Azure Active Directory를 지원합니다.

Azure Active Directory에서 리소스 소유자 비밀번호 자격 증명 플로우를 위한 애플리케이션 구성

단계 **1** Azure 포털에 로그인합니다.

단계 **2** 상단 내비게이션 바에서 **Directory+Application(**디렉토리+애플리케이션**)** 필터 아이콘을 클릭합니다. ROPC 사용 애플리케이션을 추가해야 할 Azure Active Directory 테넌트를 선택합니다.

단계 **3** 검색 창을 사용하여 **App Registrations(**앱 등록**)**를 찾아 선택합니다.

단계 **4** **+ New Registration(+** 새 등록**)**을 클릭합니다.

단계 **5** 표시되는 **Register an Application(**애플리케이션 등록**)** 창에서 **Name(**이름**)** 필드에 이 앱의 의미 있는 이름을 입력합니다.

단계 **6** **Supported account types(**지원되는 어카운트 유형**)** 영역에서 **Accounts in this organizational directory only(**이 조직 디렉토리에 있는 어카운트만**)**를 클릭합니다.

단계 **7** **Register(**등록**)**를 클릭합니다.

단계 **8** 표시되는 새 창의 왼쪽 메뉴 창에서 **Certificates & Secrets(**인증서 및 암호**)**를 클릭합니다.

단계 **9** **Client Secrets(**클라이언트 암호**)** 영역에서 **+ New Client Secret(+** 새 클라이언트 암호**)**을 클릭합니다.

단계 **10** **Add a Client Secret(**클라이언트 암호 추가**)** 대화 상자에서 **Description(**설명**)** 필드에 설명을 입력합니다.

단계 **11** **Expiry(**만료**)** 영역에서 **Never(**만료되지 않음**)**를 클릭합니다.

단계 **12** **Add(**추가**)**를 클릭합니다.

단계 **13** 클립보드에 복사 아이콘을 클릭하여 공유 암호를 복사합니다. Cisco ISE에서 ROPC 플로우를 구성할 때 이 값이 필요합니다.

단계 **14** 왼쪽 메뉴 창에서 **Overview(**개요**)**를 클릭하고, ROPC 플로우를 구성할 때 Cisco ISE에서 사용할 다음 값을 복사합니다.

- 애플리케이션(클라이언트) ID
- 디렉토리(테넌트) ID입니다

단계 **15** 이 애플리케이션에 대한 ROPC 플로우를 활성화하려면 왼쪽 메뉴 창에서 **Authentication(**인증**)**을 클릭합니다. **Advanced Settings(**고급 설정**)** 영역에서 토글 버튼이 **Yes(**예**)**로 설정되어 있는지 확인합니다.

단계 **16** 앱에 그룹 클레임을 추가하려면 왼쪽 메뉴 창에서 **Token Configuration(**토큰 컨피그레이션**)**을 클릭합니다.

단계 **17** **+ Add Groups Claim(+** 그룹 클레임 추가**)**을 클릭합니다.

단계 **18** **Edit Groups Claim(**그룹 클레임 편집**)** 대화 상자에서 **Security groups(**보안 그룹**)** 확인란을 선택합니다.

단계 **19** **Save(**저장**)**를 클릭합니다.

단계 **20** API 사용을 활성화하려면 왼쪽 메뉴 창에서 **API Permissions(API** 권한**)**를 클릭합니다.

단계 **21** **+ Add A Permission(+** 권한 추가**)**를 클릭합니다.

단계 **22** **Microsoft APIs** 영역에서 **Microsoft Graph**를 클릭합니다.

단계 **23** **Application Permissions(**애플리케이션 권한**)**를 클릭합니다.

단계 **24** **Group(**그룹**)** 드롭다운 영역에서 **Group.Read.All** 확인란을 선택합니다.

단계 **25** **Add Permissions(**권한 추가**)**를 클릭합니다.

단계 **26** **Grant Admin Consent for <user>(**<사용자>에 대해 관리자 동의 부여**)**를 클릭한 다음 **Yes(**예**)**를 클릭합니다.

Cisco ISE에서 리소스 소유자 비밀번호 자격 증명 플로우 구성

시작하기 전에

Cisco ISE GUI에서 **Menu(**메뉴**)** 아이콘(☰)을 클릭하고 **System(**시스템**)** > **Certificates(**인증서**)** > **Certificate Management(**인증서 관리**)** > **Trusted Certificates(**신뢰할 수 있는 인증서**)**를 선택합니다. **DigiCert Global Root G2**가 신뢰할 수 있는 인증서 목록에 표시되는지 확인합니다.

이 인증서가 신뢰할 수 있는 인증서 저장소에 없는 경우 PEM 형식의 공용 루트 인증서 DigiCert Global Root G2를 Cisco ISE 신뢰할 수 있는 인증서 저장소로 가져옵니다.

https://www.digicert.com/kb/digicert-root-certificates.htm을 참고하십시오.

단계 **1** Cisco ISE GUI에서 **Menu(**메뉴**)** 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **Settings(**설정**)** > **REST ID Store Settings(REST ID** 저장소 설정**)**를 선택합니다.

단계 **2** **Enabled(**활성화됨**)**를 클릭한 다음 **Submit(**제출**)**을 클릭합니다.

단계 **3** ISE 노드에서 다음 CLI 명령을 통해 REST 인증 서비스의 상태를 확인합니다.

```
show application status ise
```

REST Auth Service running(REST 인증 서비스 실행 중**)** 메시지가 응답에 표시되면 REST ID 저장소 설정이 정상적으로 활성화된 것입니다. 이제 ROPC 플로우 구성을 진행할 수 있습니다.

단계 **4** Cisco ISE GUI에서 **Menu(**메뉴**)** 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **External Identity Sources(**외부 **ID** 소스**)** > **REST(ROPC)**를 선택합니다.

단계 **5** **Add(**추가**)**를 클릭합니다.

단계 **6** 표시되는 새 창의 **Name(**이름**)** 필드에 값을 입력합니다.

단계 **7** **REST Identity Provider(REST ID** 제공자**)** 드롭다운 목록에서 구성할 ID 소스를 선택합니다.

단계 **8** 이전 작업 시 Azure Active Directory를 구성할 때 저장한 정보에서 **Client ID(**클라이언트 **ID)**, **Client Secret(**클라이언트 암호**)** 및 **Tenant ID(**테넌트 **ID)** 필드에 필요한 값을 입력합니다.

단계 **9** **Test Connection(**연결 테스트**)**을 클릭하여 Cisco ISE가 선택한 ID 소스에 연결할 수 있는지 확인합니다.

단계 **10** **Load Groups(**그룹 로드**)**를 클릭하여 연결된 ID 소스에서 사용자 그룹을 가져옵니다. 그런 다음 **Groups(**그룹**)** 드롭다운 목록에서 특정 그룹을 선택할 수 있습니다.

단계 **11** (선택 사항) 사용자 이름으로 Azure Active Directory 테넌트 사용자를 인증하려면 **Username Suffix(**사용자 이름 접미사**)** 필드에 값을 입력합니다.

예를 들어 사용자의 Azure Active Directory UPN(User Private Name)이 *example@myTest.onMicrosoft.com*인 경우 접미사는 구분 기호이고 도메인 이름은 *@myTest.onMicrosoft.com*입니다.

단계 **12** **Submit(**제출**)**을 클릭합니다.

Active Directory 다중 도메인 포리스트 지원

Cisco ISE는 다중 도메인 포리스트를 사용하는 Active Directory를 지원합니다. 각 포리스트 내의 Cisco ISE는 단일 도메인에 연결되지만 Cisco ISE가 연결된 도메인과 다른 도메인 간에 신뢰 관계가 설정된 경우에는 Active Directory 포리스트의 다른 도메인에 있는 리소스에 액세스할 수 있습니다.

Active Directory 디렉토리 서비스를 지원하는 Windows Server 운영체제 목록은 Cisco Identity Services Engine 릴리스 정보를 참고해 주십시오.

참고 Cisco ISE는 네트워크 주소 변환기 뒤에 배치되고 NAT(Network Address Translation) 주소를 사용하는 Microsoft Active Directory 서버를 지원하지 않습니다.

Active Directory와 Cisco ISE 통합을 위한 사전 요건

이 섹션에서는 Cisco ISE와 통합되도록 Active Directory를 구성하는 데 필요한 수동 단계를 설명합니다. 그러나 대부분의 경우 Cisco ISE가 Active Directory를 자동으로 구성할 수 있습니다. Active Directory와 Cisco ISE 통합의 사전 요건은 다음과 같습니다.

- Active Directory 도메인 구성을 변경하는 데 필요한 AD 도메인 관리자 자격 증명이 있어야 합니다.
- CIsco ISE에 슈퍼 관리자 또는 시스템 관리자 권한이 있어야 합니다.
- NTP(Network Time Protocol) 서버 설정을 사용하여 Cisco ISE 서버와 Active Directory 간에 시간을 동기화합니다. Cisco ISE CLI에서 NTP 설정을 구성할 수 있습니다.
- Cisco ISE는 양방향 신뢰를 가지지 않거나 서로 간에 신뢰가 없는 여러 Active Directory 도메인에 연결될 수 있습니다. 특정 조인 포인트에서 다른 도메인을 쿼리하는 경우, 액세스해야 하는 사용자 및 머신 정보가 있는 다른 도메인과 조인 포인트 간에 신뢰 관계가 존재해야 합니다. 신뢰 관계가 존재하지 않는다면 신뢰할 수 없는 도메인에 다른 조인 포인트를 생성해야 합니다. 신뢰 관계 설정에 대한 자세한 내용은 Microsoft Active Directory 설명서를 참고해 주십시오.
- Cisco ISE를 가입시키는 도메인에 Cisco ISE에서 액세스할 수 있으며 작동 가능한 글로벌 카탈로그 서버가 하나 이상 있어야 합니다.

다양한 작업을 수행하는 데 필요한 **Active Directory** 계정 권한

가입 작업	탈퇴 작업	**Cisco ISE** 머신 계정
가입 작업에는 다음 계정 권한이 필요합니다. • Active Directory 검색(Cisco ISE 머신 계정이 있는지 확인하는 용도) • 도메인에 Cisco ISE 머신 계정 생성(머신 계정이 아직 없는 경우) • 새 머신 계정에서 속성 설정(예: Cisco ISE 머신 계정 비밀번호, SPN, dnsHostname) 가입 작업을 수행하기 위해서는 반드시 도메인 관리자가 아니어도 됩니다.	탈퇴 작업에는 다음 계정 권한이 필요합니다. • Active Directory 검색(Cisco ISE 머신 계정이 있는지 확인하는 용도) • 도메인에서 Cisco ISE 머신 계정 제거 강제 탈퇴를 수행하는 경우(비밀번호 없이 탈퇴) 도메인에서 머신 계정이 제거되지 않습니다.	Active Directory 연결과의 통신에 사용되는 ISE 머신 계정에는 다음 권한이 필요합니다. • 비밀번호 변경 • 연락된 사용자 및 머신에 해당하는 사용자 및 머신 개체 읽기 • 정보(예: 신뢰할 수 있는 도메인, 대체 UPN 접미사 등)를 확인하기 위한 Active Directory 쿼리 • tokenGroups 속성 읽기 Active Directory에서 머신 계정을 미리 생성할 수 있습니다. SAM 이름이 Cisco ISE 어플라이언스 호스트 이름과 일치하는 경우 가입 작업 중에 해당 항목을 찾아서 재사용해야 합니다. 여러 가입 작업이 수행되는 경우 Cisco ISE 내에서 가입별로 하나씩 여러 머신 계정이 유지 관리됩니다.

참고 가입 또는 탈퇴 작업에 사용하는 자격 증명은 Cisco ISE에 저장되지 않습니다. 새로 생성된 Cisco ISE 머신 계정 자격 증명만 저장됩니다.

Microsoft Active Directory에서 네트워크 액세스**: SAM**에 대한 원격 호출을 허용하는 클라이언트 제한 보안 정책이 수정되었습니다. 따라서 Cisco ISE는 15일마다 머신 계정 암호를 업데이트하지 못할 수 있습니다. 머신 계정 암호가 업데이트되지 않으면 Cisco ISE는 Microsoft Active Directory를 통해 더 이상 사용자를 인증하지 않습니다. 이 이벤트에 대해 알 수 있도록 Cisco ISE 대시보드에서 **AD: ISE password update failed(AD: ISE** 비밀번호 업데이트 실패**)** 경보를 받게 됩니다.

사용자는 보안 정책을 통해 로컬 SAM(Security Accounts Manager) 데이터베이스 및 Microsoft Active Directory의 사용자 및 그룹을 열거할 수 있습니다. Cisco ISE가 머신 계정 비밀번호를 업데이트할 수 있도록 하려면 Microsoft Active Directory의 컨피그레이션이 정확한지 확인하십시오. 영향을 받는 Windows 운영체제 및 Windows 서버 버전, 네트워크에 미치는 영향 및 필요한 변경 사항에 대한 자세한 내용은 다음을 참조하십시오.

https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-access-restrict-clients-allowed-to-make-remote-sam-calls

통신을 위해 열어 두어야 하는 네트워크 포트

프로토콜	포트(원격-로컬)	대상	인증 여부	참고
DNS(TCP/UDP)	49,152 이상의 난수	DNS 서버/AD 도메인 컨트롤러	아니요	—
MSRPC	445	도메인 컨트롤러	예	—
Kerberos(TCP/UDP)	88	도메인 컨트롤러	예(Kerberos)	MS AD/KDC
LDAP(TCP/UDP)	389	도메인 컨트롤러	예	—
LDAP(GC)	3268	글로벌 카탈로그 서버	예	—
NTP	123	NTP 서버/도메인 컨트롤러	아니요	—
IPC	80	구축의 다른 ISE 노드	예(RBAC 자격 증명 사용)	—

DNS 서버

DNS 서버를 구성하는 경우 주의해야 할 사항은 다음과 같습니다.

- Cisco ISE에 구성한 DNS 서버는 사용자가 사용하려는 도메인에 대한 정방향 및 역방향 DNS 쿼리를 모두 확인할 수 있어야 합니다.
- DNS 회귀는 지연을 유발하고 심각한 성능 저하를 유발할 수 있으므로, 권한 있는 DNS 서버를 통해 Active Directory 기록 확인하는 것이 좋습니다.
- 모든 DNS 서버는 추가 사이트 정보 사용 여부와 관계없이 DC, GC 및 KDC에 대한 SRV 쿼리에 응답할 수 있어야 합니다.
- Cisco에서는 성능 향상을 위해서는 서버 IP 주소를 SRV 응답에 추가하는 것을 권장합니다.
- DNS 서버를 사용하여 공용 인터넷에 쿼리하면 안 됩니다. 이 경우 알 수 없는 이름을 확인해야 할 때 네트워크 관련 정보가 유출될 수 있습니다.

외부 ID 소스로서의 Active Directory 구성

Easy Connect나 PassiveID 작업 센터 등의 기능에 대한 구성의 일부로, Active Directory를 외부 ID 소스로 구성합니다 . 이러한 기능에 관한 자세한 내용은 Easy Connect, 81 페이지 및 PassiveID 작업 센터 , 85 페이지 항목을 참조하십시오.

Active Directory를 외부 ID 소스로 구성하는 경우 다음을 확인해 주십시오.

- Microsoft Active Directory 서버가 네트워크 주소 변환기 뒤에 배치되지 않고 NAT(Network Address Translation) 주소를 갖지 않습니다.
- 가입 작업에 사용되는 Microsoft Active Directory 계정이 유효하며 Change Password on Next Login(다음 로그인 시 비밀번호 변경)을 사용하여 구성되지 않았습니다.
- ISE에 슈퍼 관리자 또는 시스템 관리자 권한이 있습니다.

참고 Cisco ISE가 Active Directory에 연결되어 있을 때 작동 문제가 발생한다면 **Operations(**작업**)** > **Reports(**보고서**)**의 AD Connector 운영 보고서를 참조하십시오.

다음 작업을 수행하여 Active Directory를 외부 ID 소스로 구성해야 합니다.

1. Active Directory 가입 포인트를 추가하고 해당 가입 포인트에 Cisco ISE 노드 가입, 47 페이지
2. 인증 도메인 구성, 53 페이지
3. Active Directory 사용자 그룹 구성, 54 페이지
4. Active Directory 사용자 및 머신 속성 구성, 54 페이지
5. (선택사항) 비밀번호 변경, 머신 인증 및 머신 액세스 제한 설정 수정, 55 페이지

Active Directory 가입 포인트를 추가하고 해당 가입 포인트에 Cisco ISE 노드 가입

시작하기 전에

Cisco ISE 노드가 NTP 서버, DNS 서버, 도메인 컨트롤러 및 전역 카탈로그 서버가 있는 네트워크와 통신할 수 있는지 확인합니다. 도메인 진단 도구를 실행하여 이러한 매개변수를 확인할 수 있습니다.

Active Directory에 더해 Passive ID Work Center(패시브 ID 작업 센터)의 에이전트, 시스템 로그, SPAN 및 엔드포인트 프로브까지 사용하려면 조인 포인트를 생성해야 합니다.

Active Directory와 통합할 때 IPv6을 사용하려면 관련 ISE 노드에 대해 IPv6 주소를 구성했는지 확인해야 합니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **External Identity Sources(**외부 **ID** 소스**)** > **Active Directory**를 선택합니다.

단계 **2** **Add(**추가**)**를 클릭하고 **Active Directory Join Point Name(Active Directory** 가입 포인트 이름**)** 설정에서 도메인 이름과 ID 저장소 이름을 입력합니다.

단계 **3** **Submit(**제출**)**을 클릭합니다.

새로 생성하는 가입 포인트를 도메인에 가입시킬지를 묻는 팝업 메시지가 표시됩니다. 가입 포인트를 도메인에 즉시 가입시키려면 **Yes(**예**)**를 클릭합니다.

No(아니오**)**를 클릭하고 컨피그레이션을 저장하면 Active Directory 도메인 컨피그레이션이 (기본 및 보조 정책 서비스 노드에) 전역적으로 저장되지만 Cisco ISE 노드가 도메인에 가입되지는 않습니다.

단계 **4** 새로 생성한 Active Directory 가입 포인트 옆의 확인란을 선택하고 **Edit(**편집**)**를 클릭하거나 왼쪽의 탐색창에서 새 Active Directory 가입 포인트를 클릭합니다. 모든 Cisco ISE 노드, 노드 역할 및 노드 상태가 포함된 구축 가입/탈퇴 표이 표시됩니다.

단계 **5** 3단계를 진행하는 도중 가입 포인트가 도메인에 가입되지 않은 경우 관련 Cisco ISE 노드 옆의 확인란을 선택하고 **Join(**가입**)**을 클릭하여 Cisco ISE 노드를 Active Directory 도메인에 가입시킵니다.

컨피그레이션을 저장한 경우에도 이 작업을 명시적으로 수행해야 합니다. 단일 작업에서 도메인에 여러 Cisco ISE 노드를 가입시키려면 모든 가입 작업에 사용할 계정의 사용자 이름 및 비밀번호가 같아야 합니다. 각 Cisco ISE 노드를 가입시키는 데 필요한 사용자 이름 및 비밀번호가 다른 경우에는 각 Cisco ISE 노드에 대해 가입 작업을 개별적으로 수행해야 합니다.

단계 **6** **Join Domain(**도메인 가입**)** 대화 상자에서 Active Directory 사용자 이름 및 비밀번호를 입력합니다.

Store credentials(자격 증명 저장**)**는 되도록 선택하는 것이 좋습니다. 관리자의 사용자 이름이나 비밀번호가 저장되어 모니터링 용도로 구성되는 모든 DC(도메인 컨트롤러)에서 사용할 수 있습니다.

가입 작업에 사용되는 사용자는 도메인 자체에 있어야 합니다. 사용자가 다른 도메인이나 하위 도메인에 있는 경우에는 jdoe@acme.com과 같이 UPN 표기법으로 사용자 이름을 표기해야 합니다.

단계 **7** (선택 사항) **Specify Organizational Unit(**조직 단위 지정**)** 확인란을 선택합니다.

CN=Computers,DC=someDomain,DC=someTLD 이외의 특정 조직 단위에 Cisco ISE 노드 머신 계정을 배치하려는 경우 이 확인란을 선택해야 합니다. Cisco ISE는 지정된 조직 단위에 머신 계정을 생성하거나, 머신 계정이 이미 있는 경우 이 위치로 이동합니다. 조직 단위를 지정하지 않으면 Cisco ISE에서는 기본 위치를 사용합니다. 값은 완전한 DN(Distinguished Name) 형식으로 지정해야 합니다. 구문은 Microsoft 지침을 따라야 합니다. /'+,;=<> 줄 바꿈, 공백, 캐리지 리턴 등의 특수 예약 문자는 백슬래시(\)로 이스케이프 처리해야 합니다. 예를 들면 OU=Cisco ISE\,US,OU=IT Servers,OU=Servers\ 및 Workstations,DC=someDomain,DC=someTLD와 같습니다. 머신 계정이 이미 생성된 경우에는 이 확인란을 선택하지 않아도 됩니다. Active Directory 도메인에 가입한 후 머신 계정의 위치를 변경할 수도 있습니다.

단계 **8** **OK(**확인**)**를 클릭합니다.

Active Directory 도메인에 가입시킬 노드를 두 개 이상 선택할 수 있습니다.

가입 작업이 실패하면 오류 메시지가 나타납니다. 각 노드에 대한 오류 메시지를 클릭하면 해당 노드의 상세 로그를 확인할 수 있습니다.

참고 조인이 완료되면 Cisco ISE는 자신의 AD 그룹과 대응하는 보안 식별자(SID)를 업데이트합니다. Cisco ISE는 SID 업데이트 프로세스를 자동으로 시작합니다. 이 프로세스를 완료할 수 있는지를 확인해야 합니다.

참고 DNS 서비스(SRV) 레코드가 없으면 Cisco ISE를 Active Directory 도메인에 가입시키지 못할 수도 있습니다. 가입시키려는 도메인에 대해 도메인 컨트롤러가 해당 SRV 레코드를 보급하지 않기 때문입니다. 문제 해결 관련 정보는 다음 Microsoft Active Directory 설명서를 참고해 주십시오.

- http://support.microsoft.com/kb/816587
- http://technet.microsoft.com/en-us/library/bb727055.aspx

참고 ISE에는 최대 200개의 도메인 컨트롤러만 추가할 수 있습니다. 제한을 초과하면 "Error creating <DC FQDN> - Number of DCs Exceeds allowed maximum of 200(<DC FQDN> 생성 오류 - DC 수가 허용된 최대 200개를 초과)" 오류가 표시됩니다.

다음에 수행할 작업

Active Directory 사용자 그룹 구성, 54 페이지

인증 도메인을 구성합니다.

도메인 컨트롤러 추가

단계 **1** **Work Centers(**작업 센터**)** > **PassiveID(**패시브 **ID)** > **Providers(**제공자**)**를 선택하고 왼쪽 창에서 **Active Directory**를 선택합니다.

단계 **2** 생성한 Active Directory 가입 포인트 옆의 확인란을 선택하고 **Edit(**수정**)**를 클릭합니다. 모든 Cisco ISE 노드, 노드 역할 및 노드 상태가 포함된 구축 가입/탈퇴 표이 표시됩니다.

단계 **3** 참고 Passive Identity(패시브 ID) 서비스용으로 새 DC(Domain Controller)를 추가하려면 해당 DC의 로그인 자격 증명이 필요합니다.

PassiveID(패시브 ID) 탭으로 이동하여 **Add DCs(DC** 추가**)**를 클릭합니다.

단계 **4** 모니터링을 위해 조인트 포인트에 추가할 도메인 컨트롤러 옆의 확인란을 선택하고 **OK (**확인)를 클릭합니다. 도메인 컨트롤러는 PassiveID(패시브 ID) 탭의 Domain Controller(도메인 컨트롤러) 목록에 표시됩니다.

단계 **5** 도메인 컨트롤러를 구성합니다.

a) 도메인 컨트롤러에 체크 표시하고 **Edit(**수정**)**를 클릭합니다. **Edit Item(**항목 수정**)** 화면이 나타납니다.

b) 선택 사항으로, 다른 도메인 컨트롤러 필드를 수정합니다. .

c) WMI 프로토콜을 선택했다면 **Configure(**구성**)**를 클릭하여 WMI를 자동으로 구성하고 **Test(**테스트**)**를 클릭하여 연결을 테스트합니다.

DC 페일오버 메커니즘은 페일오버 시 DC가 선택되는 순서를 지정하는 DC 우선 순위 목록을 기반으로 관리됩니다. DC가 오프라인 상태이거나 오류 때문에 연결할 수 없다면 우선 순위 목록에서 우선 순위가 감소합니다. DC가 다시 온라인 상태가 되면 우선 순위 목록에서 우선 순위가 조정(중가)됩니다.

참고 Cisco ISE는 인증 플로우에 대해 읽기 전용 도메인 컨트롤러를 지원하지 않습니다.

패시브 ID용 MSRPC 프로토콜

Cisco ISE 릴리스 3.0부터는 패시브 ID에 MS-Eventing API 또는 MSRPC(Microsoft Remote Procedure Call) 프로토콜을 사용할 수 있습니다. MSRPC 프로토콜은 Cisco ISE에서 노드 통신을 설정하고 노드 간 하트비트를 모니터링하는 데 사용됩니다. WMI 프로토콜에 추가로 이 옵션을 사용할 수 있습니다.

MSRPC 프로토콜은 Cisco ISE 또는 Cisco ISE-PIC가 여러 도메인 컨트롤러에서 이벤트를 수집하거나 모니터링할 때 신뢰할 수 있는 메커니즘을 제공합니다. 또한 Active Directory 도메인 컨트롤러 사용자 로그온 이벤트의 레이턴시를 줄입니다.

Cisco ISE 3.0 이상의 경우 MSRPC가 기본 프로토콜입니다. 기본 에이전트가 설치된 서버에 장애가 발생할 경우 보조 에이전트가 활성화되어 도메인 컨트롤러를 모니터링할 수 있도록 MSPRC의 고가용성 기능을 위해 기본 에이전트와 보조 에이전트를 활성화하는 것이 좋습니다.

에이전트를 생성하는 동안 MSPRC에 독립형 옵션을 사용하도록 선택할 수도 있습니다. 그러나 독립형 에이전트를 사용하는 경우 에이전트 장애 발생 시 보조 에이전트로 대체되지 않으므로 DC 이벤트를 모니터링할 수 없습니다.

Cisco ISE 2.x에서 3.0 버전으로 업그레이드하는 동안 멤버 서버가 기존 에이전트로 업데이트되는 경우 **Agents(**에이전트**)** 창의 **Version(**버전**)** 열에 에이전트 버전이 2.0.0.1로 표시됩니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Passive ID(**패시브 **ID)** > **Providers(**제공자**)** > **Agents(**에이전트**)** .

MSRPC용 에이전트 구축

시작하기 전에

Passive Identity Service를 활성화해야 합니다. 방법은 다음과 같습니다.

Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Deployment(**구축**)**를 선택하고 구축 노드 옆의 확인란을 선택합니다. **Edit(**편집**)**를 클릭합니다. **Edit Node(**노드 편집**)** 창에서 **Enable Passive Identity Service(**패시브 **ID** 서비스 활성화**)** 확인란을 선택하고 **Save(**저장**)**를 클릭합니다.

Cisco ISE-PIC GUI에서 **Administration(**관리**)** > **System(**시스템**)** > **Deployment(**구축**)**를 선택하고 구축 노드 옆의 확인란을 선택합니다. **Edit(**편집**)**를 클릭합니다. **Edit Node(**노드 편집**)** 창에서 **Enable Passive Identity Service(**패시브 **ID** 서비스 활성화**)** 확인란을 선택하고 **Save(**저장**)**를 클릭합니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Passive ID(**패시브 **ID)** > **Providers(**제공자**)** > **Agents(**에이전트**)**.

단계 **2** **Add(**추가**)**를 클릭합니다.

단계 **3** 새 에이전트를 구축하려면 **Agents(**에이전트**)** 창에서 **Deploy New Agent(**새 에이전트 구축**)**를 클릭하고, 기존 에이전트를 등록하려면 **Register Existing Agents(**기존 에이전트 등록**)**를 클릭합니다.

Register Existing Agent(기존 에이전트 등록**)** 옵션을 선택하면 지원되지 않는 프로토콜로 인해 지원 대상인 등록된 클라이언트의 요청이 삭제될 수 있습니다. 이러한 이벤트에서는 지원되는 프로토콜로 Cisco ISE 클라이언트를 구성해야 합니다.

단계 **4** **Name(**이름**)** 필드에 에이전트 이름을 입력합니다.

단계 **5** **Host FQDN(**호스트 **FQDN)** 필드에 호스트 FQDN URL을 입력합니다.

단계 **6** **User Name(**사용자 이름**)**과 **Password(**비밀번호**)**를 입력합니다.

단계 **7** **Protocol(**프로토콜**)** 드롭다운 목록에서 **MSRPC**를 선택합니다.

단계 **8** **High Availability Settings(**고가용성 설정**)** 섹션에서 **Primary(**기본**)**를 클릭합니다.

기본 에이전트가 성공적으로 구축된 후에는 **High Availability Settings(**고가용성 설정**)** 섹션에서 **Secondary(**보조**)** 옵션을 선택해 위의 단계를 반복하여 보조 에이전트를 구축해야 합니다. 보조 에이전트를 구축하는 동안 **Primary Agent(**기본 에이전트**)** 드롭다운 목록에서, 구성된 기본 에이전트를 선택합니다.

단계 **9** **Deploy(**구축**)**를 클릭합니다.

기본 에이전트로 도메인 컨트롤러 매핑

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Passive ID(**패시브 **ID)** > **Providers(**제공자**)** > **Active Directory**.

단계 **2** **Active Directory** 창에서 **Add(**추가**)**를 클릭합니다.

단계 **3** **Connection(**연결**)** 섹션에서 도메인 컨트롤러의 **Join Point Name(**조인 포인트 이름**)** 및 **Active Directory Domain(Active Directory** 도메인**)**을 입력합니다.

단계 **4** **Submit(**제출**)**을 클릭합니다.

다음 메시지가 표시됩니다.

```
Would you like to Join all ISE Nodes to this Active Directory Domain?(모든 ISE 노드를 이 Active Directory 도메인에 조인하시겠습니까)
```

단계 **5** **Yes(**예**)**를 클릭하여 모든 ISE 노드를 조인시킵니다.

단계 **6** **Join Domain(**도메인 조인**)** 팝업 창에서 **AD User name(AD** 사용자 이름**)** 및 **Password(**비밀번호**)**를 입력합니다.

단계 **7** **Ok(**확인**)**를 클릭합니다.

단계 **8** **PassiveID(**패시브 **ID)** 탭을 클릭합니다.

단계 **9** **PassiveID Domain Controller(PassiveID** 도메인 컨트롤러**)** 창에서 매핑하려는 ISE 도메인 옆의 확인란을 클릭합니다.

다중 DC 매핑의 경우 **Use Existing Agent(**기존 에이전트 사용**)** 옵션에서 기존 에이전트를 선택할 수 있습니다.

단계 **10** **Edit(**편집**)**를 클릭합니다.

단계 **11** **Host FQDN(**호스트 **FQDN)** 필드에 호스트 FQDN URL을 입력합니다.

단계 **12** **AD User Name(AD** 사용자 이름**)** 및 **Password(**비밀번호**)** 필드에 AD 자격 증명을 입력합니다.

단계 **13** **Protocol(**프로토콜**)** 드롭다운 목록에서 **Agent(**에이전트**)**를 선택합니다.

단계 **14** **Agent(**에이전트**)** 드롭다운 목록에서 해당 에이전트(고가용성을 위한 **Primary(**기본**)** 또는 **Standalone(**독립형**)**)를 선택합니다.

단계 **15** **Save(**저장**)**를 클릭합니다.

Dashboard(대시보드**)**에서 에이전트 매핑 상태, 도메인 컨트롤러를 모니터링하는 에이전트 및 에이전트 역할을 검토할 수 있습니다. (이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **PassiveID(**패시브 **ID)** > **Overview(**개요**)**.)

Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Operations(운영)** > **RADIUS** > **Live Sessions(라이브 세션)**를 선택하여 도메인 컨트롤러 이벤트 로그를 확인합니다.

패시브 ID용 WMI 구성

시작하기 전에

AD 도메인 컨피그레이션을 변경하려면 Active Directory 도메인 관리자 자격 증명이 있어야 합니다. **Administration(관리)** > **System(시스템)** > **Deployment(구축)**에서 이 노드에 대해 패시브 ID가 활성화되었는지 확인합니다.

단계 **1** **Administration(관리)** > **Identity Management(ID 관리)** > **External Identity Sources(외부 ID 소스)** > **Active Directory**를 선택합니다.

단계 **2** 생성한 Active Directory 가입 포인트 옆의 확인란을 선택하고 **Edit(수정)**를 클릭합니다. 모든 Cisco ISE 노드, 노드 역할 및 노드 상태가 포함된 구축 가입/탈퇴 표이 표시됩니다.

단계 **3** Passive ID(패시브 ID) 탭으로 이동하여 관련 도메인 컨트롤러 옆에 있는 확인란을 선택하고 **Config WMI(WMI 구성)**를 클릭하여 ISE가 선택한 도메인 컨트롤러를 자동으로 구성하게 합니다.
Active Directory 및 도메인 컨트롤러를 수동으로 구성하거나 구성 문제를 해결하는 방법은 Active Directory와 Cisco ISE 통합을 위한 사전 요건 , 44 페이지 항목을 참조하십시오.

Active Directory 도메인 탈퇴

Active Directory 도메인 또는 이 가입 포인트에서 사용자나 머신을 더 이상 인증할 필요가 없으면, Active Directory 도메인에서 탈퇴할 수 있습니다.

명령줄 인터페이스에서 Cisco ISE 애플리케이션 컨피그레이션을 재설정하거나 백업 또는 업그레이드 이후 컨피그레이션을 복원하면 Cisco ISE는 탈퇴 작업을 수행하여 Cisco ISE 노드가 Active Directory 도메인에 이미 가입되어 있는 경우 해당 도메인에서 노드 연결을 끊습니다. 그러나 Cisco ISE 노드 계정은 Active Directory 도메인에서 제거되지 않습니다. 관리 포털에서 Active Directory 자격 증명을 사용하여 탈퇴 작업을 수행하는 것이 좋습니다. 이렇게 하면 Active Directory 도메인에서 노드 계정도 제거되기 때문입니다. Cisco ISE 호스트 이름을 변경할 때도 이 방법을 사용하는 것이 좋습니다.

시작하기 전에

Active Directory 도메인에서는 탈퇴했는데 Active Directory를 인증용 ID 소스로 계속 사용(직접 사용 또는 ID 소스 시퀀스의 일부분으로 사용)하면 인증이 실패할 수 있습니다.

단계 **1** **Administration(관리)** > **Identity Management(ID 관리)** > **External Identity Sources(외부 ID 소스)** > **Active Directory**를 선택합니다.

단계 **2** 생성한 Active Directory 조인 포인트 옆의 확인란을 선택하고 **Edit(수정)**를 클릭합니다. 모든 Cisco ISE 노드, 노드 역할 및 노드 상태가 포함된 구축 가입/탈퇴 표이 표시됩니다.

단계 **3** Cisco ISE 노드 옆의 확인란을 선택하고 **Leave(탈퇴)**를 클릭합니다.

단계 **4** Active Directory 사용자 이름 및 비밀번호를 입력하고 **OK(**확인**)**를 클릭하여 도메인을 탈퇴시킨 후 Cisco ISE 데이터베이스에서 머신 계정을 제거합니다.

Active Directory 자격 증명을 입력하는 경우 Active Directory 도메인에서 Cisco ISE 노드가 탈퇴되며 Active Directory 데이터베이스에서 Cisco ISE 머신 계정이 삭제됩니다.

참고 Active Directory 데이터베이스에서 Cisco ISE 머신 계정을 삭제하려면 여기서 입력하는 Active Directory 자격 증명에 도메인에서 머신 계정을 제거할 권한이 있어야 합니다.

단계 **5** Active Directory 자격 증명이 없는 경우에는 **No Credentials Available(**사용 가능한 자격 증명 없음**)**을 선택하고 **OK(**확인**)**를 클릭합니다.

Leave domain without credentials(자격 증명을 사용하지 않고 도메인 탈퇴**)** 확인란을 선택하면 기본 Cisco ISE 노드가 Active Directory 도메인에서 탈퇴됩니다. 이 경우에는 Active Directory 관리자가 가입 시 Active Directory에서 생성된 머신 계정을 수동으로 제거해야 합니다.

인증 도메인 구성

Cisco ISE가 가입된 도메인에서는 신뢰 관계가 설정된 다른 도메인을 확인할 수 있습니다. 기본적으로 Cisco ISE는 이러한 신뢰할 수 있는 모든 도메인에 대한 인증을 허용하도록 설정됩니다. Active Directory 구축과의 상호작용을 인증 도메인의 하위 집합으로 제한할 수 있습니다. 인증 도메인을 구성하면 선택한 도메인에 대해서만 인증이 수행되도록 각 가입 포인트에 대해 특정 도메인을 선택할 수 있습니다. 인증 도메인은 가입 포인트에서 신뢰되는 모든 도메인이 아닌 선택한 도메인의 사용자만 인증하도록 Cisco ISE에 명령하므로, 인증 도메인을 사용하는 경우 보안이 향상됩니다. 또한 인증 도메인은 검색 영역, 즉 인커밍 사용자 이름 또는 ID와 일치하는 계정을 검색하는 영역을 제한하므로 인증 요청 처리의 성능과 레이턴시도 개선됩니다. 인커밍 사용자 이름 또는 ID에는 도메인 태그(접두사 또는 접미사)가 포함되어 있지 않아야 합니다. 이러한 이유로 인해 인증 도메인을 구성하는 것이 모범 사례이므로 인증 도메인은 구성하는 것이 좋습니다.

단계 **1** **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **External Identity Sources(**외부 **ID** 소스**)** > **Active Directory**를 선택합니다.

단계 **2** **Active Directory** 조인 포인트를 클릭합니다.

단계 **3** **Authentication Domains(**인증 도메인**)** 탭을 클릭합니다.

신뢰할 수 있는 도메인 목록이 포함된 표가 표시됩니다. 기본적으로 Cisco ISE는 신뢰할 수 있는 모든 도메인에 대한 인증을 허용합니다.

단계 **4** 지정된 도메인만 허용하려면 **Use all Active Directory domains for authentication(**인증에 모든 **Active Directory** 도메인 사용**)** 확인란 선택을 취소합니다.

단계 **5** 인증을 허용할 도메인 옆의 확인란을 선택하고 **Enable Selected(**선택 항목 활성화**)**를 클릭합니다. **Authenticate(**인증**)** 열에서 이 도메인의 상태가 예로 변경됩니다.

선택한 도메인을 비활성화할 수도 있습니다.

단계 **6** 사용할 수 없는 도메인 목록을 보려면 **Show Unusable Domains(**사용할 수 없는 도메인 표시**)**를 클릭합니다. 사용할 수 없는 도메인은 단방향 신뢰, 선택적 인증 등의 이유로 인해 Cisco ISE가 인증에 사용할 수 없는 도메인입니다.

다음에 수행할 작업

Active Directory 사용자 그룹을 구성합니다.

Active Directory 사용자 그룹 구성

Active Directory 사용자 그룹을 구성해야 권한 부여 정책에서 해당 그룹을 사용할 수 있습니다. Cisco ISE는 내부적으로 SID(Security Identifiers)를 사용하여 모호한 그룹 이름 문제를 해결하고 그룹 매핑을 개선합니다. SID를 통해 정확하게 일치하는 그룹을 할당할 수 있습니다.

단계 **1** **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **External Identity Sources(**외부 **ID** 소스**)** > **Active Directory**를 선택합니다.

단계 **2** **Groups(**그룹**)** 탭을 클릭합니다.

단계 **3** 다음 중 하나를 수행합니다.

a) **Add(**추가**)** > **Select Groups From Directory(**디렉토리에서 그룹 선택**)**를 선택하여 기존 그룹을 선택합니다.

b) **Add(**추가**)** > **Add Group(**그룹 추가**)**을 선택하여 그룹을 수동으로 추가합니다. 그룹 이름과 SID를 모두 입력하거나, 그룹 이름만 입력하고 **Fetch SID(SID** 가져오기**)**를 누를 수 있습니다.

사용자 인터페이스 로그인 시 그룹 이름에 큰따옴표(")를 사용하지 마십시오.

단계 **4** 그룹을 수동으로 선택하는 경우 필터를 사용하여 그룹을 검색할 수 있습니다. 예를 들어 필터 기준으로 **admin***를 입력하고 **Retrieve Groups(**그룹 검색**)**를 클릭하면 admin으로 시작하는 사용자 그룹을 확인할 수 있습니다. 별표(*) 와일드카드 문자를 입력하여 결과를 필터링할 수도 있습니다. 그룹은 한 번에 500개만 검색할 수 있습니다.

단계 **5** 권한 부여 정책에서 사용 가능하도록 지정할 그룹 옆의 확인란을 선택하고 **OK(**확인**)**를 클릭합니다.

단계 **6** 그룹을 수동으로 추가하도록 선택하는 경우 새 그룹의 이름과 SID를 입력합니다.

단계 **7** **OK(**확인**)**를 클릭합니다.

단계 **8** **Save(**저장**)**를 클릭합니다.

참고 그룹을 삭제하고 원본과 같은 이름으로 새 그룹을 생성하는 경우에는 **Update SID Values(SID** 값 업데이트**)**를 클릭하여 새로 생성한 그룹에 새 SID를 할당해야 합니다. 업그레이드 후 처음으로 가입하고 나면 SID가 자동으로 업데이트됩니다.

다음에 수행할 작업

Active Directory 사용자 속성을 구성합니다.

Active Directory 사용자 및 머신 속성 구성

Active Directory 사용자 및 머신 속성을 구성해야 권한 부여 정책의 조건에서 해당 속성을 사용할 수 있습니다.

단계 **1** **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **External Identity Sources(**외부 **ID** 소스**)** > **Active Directory**를 선택합니다.

단계 **2** **Attributes(**속성**)** 탭을 클릭합니다.

단계 **3** **Add(**추가**)** > **Add Attribute(**속성 추가**)**를 클릭하여 속성을 수동으로 추가하거나 **Add(**추가**)** > **Select Attributes From Directory(**디렉터리에서 속성 선택**)**를 선택하여 디렉터리에서 속성 목록을 선택합니다.

Cisco ISE에서는 속성 유형 IP를 수동으로 추가할 때 사용자 인증에 IPv4 또는 IPv6 주소를 사용하도록 AD를 구성할 수 있습니다.

단계 **4** 디렉터리에서 속성을 추가하도록 선택하는 경우 **Sample User or Machine Account(**샘플 사용자 또는 머신 계정**)** 필드에 사용자의 이름을 입력하고 **Retrieve Attributes(**속성 검색**)**를 클릭하여 사용자에 대한 속성 목록을 가져옵니다. 예를 들어 관리자 속성 목록을 가져오려면 **administrator(**관리자**)**를 입력합니다. 별표(*) 와일드카드 문자를 입력하여 결과를 필터링할 수도 있습니다.

참고 예시 사용자 이름을 입력할 때는 Cisco ISE에 연결되는 Active Directory 도메인에 속한 사용자를 선택해야 합니다. 머신 속성을 얻고자 예시 머신을 선택할 때는 머신 이름 앞에 'host/'를 붙이거나 SAM$ 형식을 사용해야 합니다. 예를 들어 host/myhost를 사용할 수 있습니다. 속성을 검색할 때 표시되는 예제 값은 설명을 위해서만 제공되는 것이며 저장되지 않습니다.

단계 **5** 선택하려는 Active Directory의 속성 옆에 있는 확인란을 선택하고 **OK(**확인**)**를 클릭합니다.

단계 **6** 속성을 수동으로 추가하도록 선택하는 경우 새 속성의 이름을 입력합니다.

단계 **7** **Save(**저장**)**를 클릭합니다.

비밀번호 변경, 머신 인증 및 머신 액세스 제한 설정 수정

시작하기 전에

Active Directory 도메인에 Cisco ISE를 가입시켜야 합니다. 자세한 내용은 Active Directory 가입 포인트를 추가하고 해당 가입 포인트에 Cisco ISE 노드 가입, 47 페이지를 참고하십시오.

단계 **1** **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **External Identity Sources(**외부 **ID** 소스**)** > **Active Directory**를 선택합니다.

단계 **2** Cisco ISE 노드 옆의 확인란을 선택하고 **Edit(**수정**)**를 클릭합니다 .

단계 **3** **Advanced Settings(**고급 설정**)** 탭을 클릭합니다.

단계 **4** 비밀번호 변경, 머신 인증 및 MAR(Machine Access Restrictions) 설정을 필요한 대로 수정합니다.

단계 **5** 인증 또는 쿼리 중에 사용자의 다이얼인 권한을 확인하려면 **Enable dial-in check(**다이얼인 확인 활성화**)** 확인란을 선택합니다. 다이얼인 권한이 거부되는 경우 확인 결과에 따라 인증이 거부될 수 있습니다.

단계 **6** 인증 또는 쿼리 중에 서버가 사용자를 다시 호출하게 하려면 **Enable callback check for dial-in clients(**다이얼인 클라이언트용 콜백 확인 활성화**)** 확인란을 선택합니다. 서버에서 사용하는 IP 주소 또는 전화 번호는 발신자나 네트워크 관리자가 설정할 수 있습니다. 확인 결과는 RADIUS 응답의 장치로 반환됩니다.

단계 **7** 일반 텍스트 인증에 Kerberos를 사용하려는 경우 **Use Kerberos for Plain Text Authentications(**일반 텍스트 인증에 **Kerberos** 사용**)** 확인란을 선택합니다. 기본 및 권장 옵션은 MS-RPC입니다.

MAR(머신 액세스 제한) 캐시

애플리케이션 서비스를 수동으로 중지하면 Cisco ISE는 MAR 캐시 콘텐츠, 호출 스테이션 ID 목록 및 해당하는 타임스탬프를 로컬 디스크의 파일에 저장합니다. 런타임 서비스를 실수로 재시작하는 경우 Cisco ISE는 인스턴스의 MAR 캐시 엔트리를 저장하지 않습니다. Cisco ISE는 애플리케이션 서비스가 재시작될 때 캐시 엔트리 TTL(Time to Live)을 기준으로 하여 로컬 디스크의 파일에서 MAR 캐시 엔트리를 읽습니다. 재시작 후 애플리케이션 서비스가 작동하면 Cisco ISE는 해당 인스턴스의 현재 시간을 MAR 캐시 엔트리 시간과 비교합니다. 현재 시간과 MAR 엔트리 시간 사이의 차이가 MAR 캐시 엔트리 TTL(Time to Live)보다 크면 Cisco ISE는 디스크에서 해당 엔트리를 검색하지 않습니다. 그렇지 않은 경우 Cisco ISE는 해당 MAR 캐시 엔트리를 검색하고 MAR 캐시 엔트리 TTL(Time to Live)을 업데이트합니다.

MAR 캐시를 구성하는 방법

외부 ID 소스에 정의된 Active Directory의 **Advanced Settings(**고급 설정**)** 탭에서 다음 옵션이 선택되었는지 확인합니다.

- **Enable Machine Authentication(**머신 인증 활성화**)**: 머신 인증을 활성화합니다.
- **Enable Machine Access Restriction(**머신 액세스 제한 활성화**)**: 권한 부여 전에 사용자 및 머신 인증을 결합합니다.

MAR 캐시를 권한 부여에 사용하는 방법

권한 부여 정책에서 `WasMachineAuthenticated is True`를 사용합니다. 이 규칙과 자격 증명 규칙을 사용하여 이중 인증을 수행할 수 있습니다. 머신 인증은 AD 자격 증명보다 먼저 수행해야합니다.

System(시스템**) > Deployment(**구축**)** 페이지에서 노드 그룹을 생성 한 경우 MAR Cache Distribution(MAC 캐시 배포)을 활성화합니다. MAR 캐시 배포는 MAR 캐시를 동일한 노드 그룹의 모든 PSN에 복제합니다.

추가 정보

다음 Cisco ISE 커뮤니티 페이지를 참조하십시오.

- https://community.cisco.com/t5/policy-and-access/mar-why-is-it-useful/td-p/3213527
- https://community.cisco.com/t5/policy-and-access/ise-2-1-mar-aging-time-eap-tls/td-p/3209628

관련 항목

외부 ID 소스로서의 Active Directory 구성, 46 페이지

사용자 맞춤화 스키마 구성

시작하기 전에

Active Directory 도메인에 Cisco ISE를 가입시켜야 합니다.

단계 **1** **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **External Identity Sources(**외부 **ID** 소스**)** > **Active Directory**를 선택합니다.

단계 **2** 가입 포인트를 선택합니다.

단계 **3** **Advanced Settings(**고급 설정**)** 탭을 클릭합니다.

단계 **4** **Schema(**스키마**)** 섹션의 **Schema(**스키마**)** 드롭다운 목록에서 **Custom(**맞춤화**)** 옵션을 선택합니다. 필요에 따라 사용자 정보 속성을 업데이트할 수 있습니다. 이러한 속성은 이름, 성, 이메일, 전화, 지역 등의 사용자 정보를 수집하는 데 사용됩니다.

사전 정의된 속성은 Active Directory 스키마(구축 당시 기본으로 내장된 스키마)에 사용됩니다. 사전 정의된 스키마의 속성을 편집하면 Cisco ISE가 자동으로 사용자 맞춤화 스키마를 생성합니다.

Active Directory 다중 가입 컨피그레이션 지원

Cisco ISE는 여러 Active Directory 도메인에 대한 다중 가입을 지원합니다. Cisco ISE는 최대 50개의 Active Directory 가입을 지원합니다. Cisco ISE는 양방향 신뢰를 가지지 않거나 서로 간에 신뢰가 없는 여러 Active Directory 도메인에 연결될 수 있습니다. Active Directory 다중 도메인 가입은 각 가입마다 일련의 개별 Active Directory 도메인과 함께 고유한 그룹, 속성 및 권한 부여 정책으로 구성됩니다.

동일한 포리스트에 여러 번 가입할 수 있습니다. 즉, 필요한 경우 동일 포리스트의 여러 도메인에 가입할 수 있습니다.

Cisco ISE는 이제 단방향 신뢰를 통한 도메인 가입을 지원합니다. 이 옵션을 사용하면 단방향 신뢰로 인해 발생하는 권한 문제를 피할 수 있습니다. 신뢰할 수 있는 도메인에 가입하여 양쪽 도메인을 모두 볼 수 있습니다.

- 가입 포인트: Cisco ISE에서 Active Directory 도메인에 대한 각각의 개별적 가입을 가입 포인트라고 합니다. Active Directory 가입 포인트는 Cisco ISE ID 저장소이며 인증 정책에 사용될 수 있습니다. 속성 및 그룹에 대한 사전이 연결되어 있으며, 이는 권한 부여 조건에 사용될 수 있습니다.
- 범위: 함께 그룹화된 Active Directory 가입 포인트의 하위 집합을 범위라고 합니다. 인증 정책에서 인증 결과로 단일 가입 포인트 대신 범위를 사용할 수 있습니다. 범위는 여러 가입 포인트에 대해 사용자를 인증하는 데 사용됩니다. 가입 포인트마다 여러 규칙을 사용하는 대신, 범위를 사용하면 단일 규칙으로 동일한 정책을 생성할 수 있으므로 요청을 처리하는 시간을 절약하고 성능을 높일 수 있습니다. 가입 포인트는 여러 범위로 존재할 수 있습니다. 범위는 ID 소스 시퀀스에 포함될 수 있습니다. 범위에는 사전이 연결되어 있지 않으므로 권한 부여 정책 조건에서 범위를 사용할 수 없습니다.

Cisco ISE를 새로 설치하는 경우 기본적으로 범위가 존재하지 않습니다. 이를 범위 없음 모드라고 합니다. 범위를 추가하면 Cisco ISE가 다중 범위 모드로 진입합니다. 필요한 경우 범위 없음 모드로 복귀할 수 있습니다. 모든 가입 포인트는 Active Directory 폴더로 이동합니다.

- Initial_Scope는 범위 없음 모드에서 추가된 Active Directory 가입 포인트를 저장하는 데 사용되는 암시적 범위입니다. 다중 범위 모드가 활성화되면 모든 Active Directory 가입 포인트가 자동으로 생성된 Initial_Scope로 이동합니다. Initial_Scope의 이름을 변경할 수 있습니다.
- All_AD_Instances는 Active Directory 컨피그레이션에 표시되지 않는 내장형 의사 범위입니다. 이는 정책 및 ID 시퀀스에서 인증 결과로 표시되는 유일한 항목입니다. Cisco ISE에 구성된 모든 Active Directory 가입 포인트를 선택하려는 경우 이 범위를 선택할 수 있습니다.

Active Directory 가입 포인트를 추가할 새 범위 생성

단계 **1** **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **External Identity Sources(**외부 **ID** 소스**)** > **Active Directory**를 선택합니다.

단계 **2** **Scope Mode(**범위 모드**)**를 클릭합니다.
Initial_Scope라는 기본 범위가 생성되며 현재 가입 포인트가 모두 이 스코프에 배치됩니다.

단계 **3** 범위를 더 생성하려면 **Add(**추가**)**를 클릭합니다.

단계 **4** 새 범위의 이름과 설명을 입력합니다.

단계 **5** **Submit(**제출**)**을 클릭합니다.

ID 다시 쓰기

ID 다시 쓰기는 ID가 외부 Active Directory 시스템으로 전달되기 전에 해당 ID를 조작하도록 Cisco ISE에 지시하는 고급 기능입니다. ID를 원하는 형식으로 변경하는 규칙을 생성하여 도메인 접두사 및/또는 접미사 또는 선택한 다른 추가 마크업을 포함하거나 제외시킬 수 있습니다.

ID 다시 쓰기 규칙은 클라이언트로부터 받은 사용자 이름 또는 호스트 이름에 적용됩니다. 그런 다음 그러한 이름은 주체 검색, 인증 및 권한 부여 쿼리와 같은 작업에 사용되도록 Active Directory로 전달됩니다. Cisco ISE는 조건 토큰과 일치시키고 첫 번째 일치 항목이 발견되면 Cisco ISE는 정책 처리를 중단하고 결과에 따라 ID 문자열을 다시 씁니다.

다시 쓰는 동안 대괄호 [ ]로 묶인 모든 항목(예: [IDENTITY])은 평가 측에서 평가되지 않지만 그 대신 문자열의 해당 위치와 일치하는 문자열이 추가되는 변수입니다. 대괄호가 없는 항목은 평가 측과 규칙을 다시 쓰기 측 모두에서 고정 문자열로 평가됩니다.

다음은 몇 가지 ID 다시 쓰기 사례로, 사용자가 ACME\jdoe를 ID로 입력한다고 가정합니다.

- ID가 **ACME\[IDENTITY]**와 일치하는 경우 **[IDENTITY]**로 다시 씁니다.

  결과는 jdoe가 됩니다. 이 규칙은 모든 사용자 이름에서 ACME 접두사를 제거하도록 Cisco ISE에 지시합니다.

- ID가 **ACME\[IDENTITY]**와 일치하는 경우 **[IDENTITY]@ACME.com**으로 다시 씁니다.

결과는 jdoe@ACME.com이 됩니다. 이 규칙은 접미사 표기법의 접두사 형식 또는 NetBIOS 형식을 UPN 형식으로 변경하도록 Cisco ISE에 지시합니다.

- ID가 **ACME\[IDENTITY]**와 일치하는 경우 **ACME2\[IDENTITY]**로 다시 씁니다.

  결과는 ACME2\jdoe가 됩니다. 이 규칙은 특정 접두사를 가진 모든 사용자 이름을 대체 접두사로 변경하도록 Cisco ISE에 지시합니다.

- ID가 **[ACME]\jdoe.USA**와 일치하는 경우 **[IDENTITY]@[ACME].com**으로 다시 씁니다.

  결과는 jdoe\ACME.com이 됩니다. 이 규칙은 점 뒤의 영역(이 경우, 국가)을 제거하고 올바른 도메인으로 대체하도록 ISE에 지시합니다.

- ID가 **E=[IDENTITY]**와 일치하는 경우 **[IDENTITY]**로 다시 씁니다.

  결과는 jdoe가 됩니다. 이 예제 규칙은 ID를 인증서에서 가져오고, 필드가 이메일 주소이며, 주체별로 검색하도록 Active Directory가 구성된 경우에 생성될 수 있습니다. 이 규칙은 Cisco ISE에 'E='를 제거하도록 지시합니다.

- ID가 **E=[EMAIL],[DN]**과 일치하는 경우 **[DN]**으로 다시 씁니다.

  이 규칙은 인증서 주체를 E=jdoe@acme.com, CN=jdoe, DC=acme, DC=com에서 pure DN, CN=jdoe, DC=acme, DC=com으로 변환합니다. 이 예제 규칙은 ID를 인증서 주체에서 가져오고 DN을 기준으로 사용자를 검색하도록 Active Directory가 구성된 경우에 생성될 수 있습니다. 이 규칙은 이메일 접두사를 제거하고 DN을 생성하도록 Cisco ISE에 지시합니다.

다음은 ID 다시 쓰기 규칙을 작성하는 동안 흔히 하는 몇 가지 실수입니다.

- ID가 **[DOMAIN]\[IDENTITY]**와 일치하는 경우 **[IDENTITY]@DOMAIN.com**으로 다시 씁니다.

  결과는 jdoe@DOMAIN.com이 됩니다. 이 규칙은 규칙 다시 쓰기 측에서 [DOMAIN]이 대괄호 [ ]로 묶이지 않았습니다.

- ID가 **DOMAIN\[IDENTITY]**와 일치하는 경우 **[IDENTITY]@[DOMAIN].com**으로 다시 씁니다.

  여기서는 결과가 다시 jdoe@DOMAIN.com이 됩니다. 이 규칙은 규칙 평가 측 [DOMAIN]이 대괄호 [ ]로 묶이지 않았습니다.

ID 다시 쓰기 규칙은 Active Directory 가입 지점 관점에서 항상 적용됩니다. 인증 정책의 결과로 특정 범위를 선택한 경우에도 각 Active Directory 가입 지점에 다시 쓰기 규칙이 적용됩니다. EAP-TLS가 사용 중인 경우 인증서에서 가져온 ID에도 이러한 다시 쓰기 규칙이 적용됩니다.

ID 재작성 활성화

참고 이 컨피그레이션 작업은 선택 사항입니다. 이 작업을 수행하면 모호한 ID 오류 등의 여러 원인으로 인해 발생할 수 있는 인증 실패를 줄일 수 있습니다.

시작하기 전에

Active Directory 도메인에 Cisco ISE를 가입시켜야 합니다.

단계 **1** **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **External Identity Sources(**외부 **ID** 소스**)** > **Active Directory**를 선택합니다.

단계 **2** **Advanced Settings(**고급 설정**)** 탭을 클릭합니다.

단계 **3** **Identity Rewrite(ID** 재작성**)** 섹션에서 재작성 규칙을 적용하여 사용자 이름을 수정할지 여부를 선택합니다.

단계 **4** 일치 조건과 재작성 결과를 입력합니다. 표시되는 기본 규칙을 제거하고 요건에 따라 규칙을 입력할 수 있습니다. Cisco ISE는 정책을 순서대로 처리하며, 요청 사용자 이름과 일치하는 첫 번째 조건이 적용됩니다. 일치하는 토큰(대괄호 안의 텍스트)을 사용하여 원래 사용자 이름의 요소를 결과로 전송할 수 있습니다. 일치하는 규칙이 없으면 ID 이름은 변경되지 않고 그대로 유지됩니다. **Launch Test(**테스트 시작**)** 버튼을 클릭하여 재작성 처리를 미리 볼 수 있습니다.

ID 확인 설정

일부 ID 유형에는 접두사 또는 접미사와 같은 도메인 마크업이 포함되어 있습니다. 예를 들어 NetBIOS ID(예: ACME\jdoe) "ACME"는 UPN ID(예: jdoe@acme.com)에서와 마찬가지로 도메인 마크업 접두사이며, "acme.com"은 도메인 마크업 접미사입니다. 도메인 접두사는 조직 내 Active Directory 도메인의 NetBIOS(NTLM) 이름과 일치해야 하고 도메인 접미사는 Active Directory 도메인의 DNS 이름 또는 조직 내 대체 UPN 접미사와 일치해야 합니다. 예를 들어 gmail.com은 Active Directory 도메인의 DNS 이름이 아니므로 jdoe@gmail.com은 도메인 마크업 없이 처리됩니다.

ID 확인 설정을 사용하면 Active Directory 구축에 맞게 보안과 성능 사이에서 균형을 유지하도록 중요한 설정을 구성할 수 있습니다. 이러한 설정을 사용하여 도메인 마크업 없이 사용자 이름 및 호스트 이름에 대한 인증을 조정할 수 있습니다. Cisco ISE가 사용자 도메인을 인식하지 못하는 경우 모든 인증 도메인에서 사용자를 검색하도록 구성할 수 있습니다. 사용자가 한 도메인에서 발견되는 경우에도 Cisco ISE는 ID 모호성이 발생하지 않도록 모든 응답을 기다립니다. 이 프로세스는 도메인 수, 네트워크 레이턴시, 로드 등에 따라 오랜 시간이 소요될 수 있습니다.

ID 확인 문제 방지

인증 중에 사용자 및 호스트에 대한 정규화된 이름(즉, 도메인 마크업이 포함된 이름)을 사용하는 것이 좋습니다. 예를 들어 사용자의 경우 UPN 및 NetBIOS 이름을 사용하고 호스트의 경우 FQDN을 사용합니다. 이는 특히 들어오는 사용자 이름에 대한 여러 Active Directory 계정 일치(예: jdoe는 jdoe@emea.acme.com 및 jdoe@amer.acme.com과 일치함)와 같이 모호성 오류가 자주 발생하는 경우에 중요합니다. 경우에 따라 정규화된 이름을 사용하는 것이 유일한 문제 해결 방법일 수 있습니다. 다른 경우에는 사용자의 고유한 비밀번호를 사용하는 것만으로도 충분할 수 있습니다. 따라서 처음부터 고유 ID를 사용하면 효율성을 높이고 비밀번호 잠금 문제를 줄일 수 있습니다.

ID 확인 설정 구성

참고 이 컨피그레이션 작업은 선택 사항입니다. 이 작업을 수행하면 모호한 ID 오류 등의 여러 원인으로 인해 발생할 수 있는 인증 실패를 줄일 수 있습니다.

시작하기 전에

Active Directory 도메인에 Cisco ISE를 가입시켜야 합니다.

단계 **1** **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **External Identity Sources(**외부 **ID** 소스**)** > **Active Directory**를 선택합니다.

단계 **2** **Advanced Settings(**고급 설정**)** 탭을 클릭합니다.

단계 **3** **Identity Resolution(ID** 확인**)** 섹션에서 사용자 이름 또는 머신 이름에 대한 ID 확인을 위해 다음 설정을 정의합니다. 이 설정은 사용자 검색 및 인증을 위한 고급 컨트롤을 제공합니다.

첫 번째 설정은 태그가 없는 ID용입니다. 이 경우에는 다음 옵션 중에서 선택할 수 있습니다.

- **Reject the request(**요청 거부**)**: 이 옵션을 사용하는 경우 SAM 이름 등의 도메인 태그가 없는 사용자의 인증이 실패합니다. Cisco ISE가 가입된 모든 글로벌 카탈로그에서 ID를 조회해야 하므로 안전하지 않을 수도 있는 다중 가입 도메인의 경우 이 옵션이 유용합니다. 이 옵션을 선택하면 사용자는 도메인 태그가 있는 이름을 사용해야 합니다.
- **Only search in the "Authentication Domains" from the joined forest(**조인된 포리스트의 "인증 도메인"만 검색**)**: 이 옵션을 사용하는 경우 인증 도메인 섹션에 지정되어 있는 조인 포인트의 포리스트 내 도메인에서만 ID를 검색합니다. 이 옵션은 기본값이며, SAM 계정 이름에 대한 Cisco ISE 1.2의 동작과 동일합니다.
- **Search in all the "Authentication Domains" sections(**모든 "인증 도메인" 섹션 검색**)**: 이 옵션을 사용하는 경우 신뢰할 수 있는 모든 포리스트 내 모든 인증 도메인에서 ID를 검색합니다. 따라서 레이턴시가 길어지고 성능이 저하될 수 있습니다.

Cisco ISE에서 인증 도메인이 구성되어 있는 방법에 따라 적절한 옵션을 선택합니다. 특정 인증 도메인만 선택하는 경우, 즉 두 번째 옵션과 세 번째 옵션을 선택하는 경우에는 해당 도메인만 검색합니다.

Cisco ISE가 "인증 도메인" 섹션에 지정된 컨피그레이션을 준수하기 위해 필요한 모든 GC(Global Catalogs)와 통신할 수 없는 경우에는 두 번째 설정이 사용됩니다. 이 경우에는 다음 옵션 중에서 선택할 수 있습니다.

- **Proceed with available domains(**사용 가능한 도메인으로 인증 진행**)**: 이 옵션을 사용하는 경우 사용 가능한 도메인 중에서 일치 항목을 찾으면 인증이 진행됩니다.
- **Drop the request(**요청 삭제**)**: 이 옵션을 사용하는 경우 ID 확인 과정에서 연결할 수 없거나 사용할 수 없는 도메인이 발견되면 인증 요청이 삭제됩니다.

Active Directory Authentication(인증)용 Test Users(사용자 테스트)

Test User(사용자 테스트) 도구를 사용하여 Active Directory에서 사용자 인증을 확인할 수 있습니다. 그룹과 속성을 가져와 검토할 수도 있습니다. 단일 가입 포인트 또는 범위에 대해 테스트를 실행할 수 있습니다.

단계 **1** **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **External Identity Sources(**외부 **ID** 소스**)** > **Active Directory**를 선택합니다.

단계 **2** 다음 옵션 중 하나를 선택합니다.

- 모든 가입 포인트에서 테스트를 실행하려면 **Advanced Tools(**고급 도구**)** > **Test User for All Join Points(**모든 가입 포인트에 대해 사용자 테스트**)**를 선택합니다.
- 특정 가입 포인트에 대해 테스트를 실행하려면 해당 가입 포인트를 선택하고 **Edit(**편집**)**를 클릭합니다. Cisco ISE 노드를 선택하고 **Test User(**사용자 테스트**)**를 클릭합니다.

단계 **3** Active Directory에서 사용자 또는 호스트의 사용자 이름 및 비밀번호를 입력합니다.

단계 **4** 인증 유형을 선택합니다. Lookup(조회) 옵션을 선택하는 경우에는 3단계에서 비밀번호를 입력하지 않아도 됩니다.

단계 **5** 모든 가입 포인트에 이 테스트를 실행하는 경우 이 테스트를 실행할 Cisco ISE 노드를 선택합니다.

단계 **6** Active Directory에서 그룹과 속성을 검색하고 싶다면 Retrieve Groups and Attributes(그룹과 속성 가져오기) 확인란을 선택합니다.

단계 **7** **Test(**테스트**)**를 클릭합니다.
테스트 작업의 결과 및 단계가 표시됩니다. 이러한 단계를 통해 실패 이유 및 문제 해결 상황을 파악할 수 있습니다.

Active Directory에서 각 처리 단계(인증, 조회 또는 그룹/속성 가져오기)를 수행하는 데 걸린 시간(밀리초)을 볼 수도 있습니다. 작업을 수행한 시간이 임계값을 초과하면 Cisco ISE에서 경고 메시지가 표시됩니다.

Active Directory 컨피그레이션 삭제

Active Directory 외부 ID 소스로 사용하지 않으려는 경우 Active Directory 컨피그레이션을 삭제해야 합니다. 다른 Active Directory 도메인에 가입하려는 경우에는 컨피그레이션을 삭제하지 마십시오. 현재 가입되어 있는 도메인은 그대로 두고 새 도메인에 가입할 수 있습니다.

시작하기 전에

Active Directory 도메인이 남아 있는지 확인합니다.

단계 **1** **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **External Identity Sources(**외부 **ID** 소스**)** > **Active Directory**를 선택합니다.

단계 **2** 구성되어 있는 Active Directory 옆의 확인란을 선택합니다.

단계 **3** 로컬 노드 상태가 가입되지 않음으로 나열되어 있는지 확인합니다.

단계 **4** **Delete(**삭제**)**를 클릭합니다.

Active Directory 데이터베이스에서 컨피그레이션이 제거되었습니다. 나중에 Active Directory를 사용하려는 경우 유효한 Active Directory 컨피그레이션을 다시 제출하면 됩니다.

노드의 Active Directory 가입 보기

Node View(노드 보기**)** 버튼(**Active Directory** 페이지)을 사용하면 지정된 Cisco ISE 노드에 대한 모든 Active Directory 가입 포인트의 상태나 모든 Cisco ISE 노드의 모든 가입 포인트를 확인할 수 있습니다.

단계 **1** **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **External Identity Sources(**외부 **ID** 소스**)** > **Active Directory**를 선택합니다.

단계 **2** **Node View(**노드 보기**)**를 클릭합니다.

단계 **3** **ISE Node(ISE** 노드**)** 드롭다운 목록에서 노드를 선택합니다.
표에 노드별 Active Directory 상태가 나열됩니다. 구축에 가입 포인트와 Cisco ISE 노드가 여러 개 있는 경우 이 표이 업데이트되는 데 몇 분 정도 걸릴 수 있습니다.

단계 **4** 가입 포인트 **Name(**이름**)** 링크를 클릭하여 해당 Active Directory 가입 포인트로 이동한 후에 다른 특정 작업을 수행합니다.

단계 **5** **Diagnostic Summary(**진단 요약**)** 열에 있는 링크를 클릭하여 **Diagnostic Tools(**진단 도구**)** 페이지로 이동한 후에 특정 문제를 해결합니다. 진단 도구에는 노드당 각 가입 포인트에 대한 최신 진단 결과가 표시됩니다.

Active Directory 문제 진단

Diagnostic Tool(진단 도구)은 모든 Cisco ISE 노드에서 실행되는 서비스입니다. Active Directory 구축을 자동으로 테스트 및 진단할 수 있으며, 테스트 집합을 실행하여 Cisco ISE에서 Active Directory를 사용할 때 기능 또는 성능 오류를 발생시킬 수 있는 문제를 탐지할 수 있습니다.

Cisco ISE는 여러 이유로 Active Directory에 가입하거나 인증하지 못할 수 있습니다. 이 도구를 사용하면 Cisco ISE를 Active Directory에 연결하기 위한 사전 요건을 올바르게 구성할 수 있습니다. 그리고 네트워킹, 방화벽 컨피그레이션, 클록 동기화, 사용자 인증 등의 문제를 탐지할 수 있습니다. 이 도구는 단계별 설명서 방식으로 작동하며, 필요한 경우 중간에 모든 레이어의 문제를 해결할 수 있습니다.

단계 **1** **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **External Identity Sources(**외부 **ID** 소스**)** > **Active Directory**를 선택합니다.

단계 **2** **Advanced Tools(**고급 도구**)** 드롭다운을 클릭하고 **Diagnostic Tools(**진단 도구**)**를 선택합니다.

단계 **3** 진단을 실행할 Cisco ISE 노드를 선택합니다.

Cisco ISE 노드를 선택하지 않으면 모든 노드에서 테스트가 실행됩니다.

단계 **4** 특정 Active Directory 가입 포인트를 선택합니다.

Active Directory 가입 포인트를 선택하지 않으면 모든 가입 포인트에서 테스트가 실행됩니다.

단계 **5** 진단 보고서는 온디맨드 또는 예약 방식으로 실행할 수 있습니다.

- 테스트를 즉시 실행하려면 **Run Tests Now(**지금 테스트 실행**)**를 선택합니다.
- 예약된 간격으로 테스트를 실행하려면 **Run Scheduled Tests(**예약된 테스트 실행**)** 확인란을 선택하여 테스트를 실행할 시작 시간과 간격(시간, 일 또는 주)을 지정합니다. 이 옵션을 활성화하면 모든 진단 테스트가 모든 노드 및 인스턴스에서 실행되며, **Home(**홈**)** 대시보드의 **Alarms(**경보**)** 데슬렛에서 장애가 보고됩니다.

단계 6 **View Test Details(**테스트 세부정보 보기**)**를 클릭하여 Warning(경고) 또는 Failed(장애) 상태의 테스트에 대한 세부 정보를 확인합니다.
이 표을 참조하여 특정 테스트를 다시 실행하고, 실행 중인 테스트를 중지하고, 특정 테스트의 보고서를 확인할 수 있습니다.

Active Directory 디버그 로그 활성화

Active Directory 디버그 로그는 기본적으로 기록되지 않습니다. 구축에서 정책 서비스 페르소나로 지정된 Cisco ISE 노드에 대해 이 옵션을 활성화해야 합니다. Active Directory 디버그 로그를 활성화하는 경우 ISE 성능에 영향을 줄 수 있습니다.

단계 1 **Administration(**관리**)** > **System(**시스템**)** > **Logging(**로깅**)** > **Debug Log Configuration(**디버그 로그 컨피그레이션**)**을 선택합니다.

단계 2 Active Directory 디버그 정보를 가져올 Cisco ISE Policy Service(정책 서비스) 노드 옆의 라디오 버튼을 클릭하고 **Edit(**수정**)**를 클릭합니다.

단계 3 **Active Directory** 라디오 버튼을 클릭하고 **Edit(**수정**)**를 클릭합니다.

단계 4 Active Directory 옆의 드롭다운 목록에서 **DEBUG**를 선택합니다. 여기에는 오류, 경고 및 자세한 정보 표시 로그가 포함됩니다. 전체 로그를 가져오려면 **TRACE**를 선택합니다.

단계 5 **Save(**저장**)**를 클릭합니다.

문제 해결을 위해 Active Directory 로그 파일 가져오기

발생했을 수 있는 문제를 해결하려면 Active Directory 디버그 로그를 다운로드하여 확인합니다.

시작하기 전에

Active Directory 디버그 로깅을 활성화해야 합니다.

단계 1 **Operations(**운영**)** > **Troubleshoot(**문제 해결**)** > **Download Logs(**로그 다운로드**)**를 선택합니다.

단계 2 Active Directory 디버그 로그 파일을 가져올 노드를 클릭합니다

단계 3 **Debug Logs(**디버그 로그**)** 탭을 클릭합니다.

단계 4 이 페이지를 스크롤하여 ad_agent.log 파일을 찾습니다. 이 파일을 클릭하여 다운로드합니다.

Active Directory 경보 및 보고서

Cisco ISE는 Active Directory 관련 활동을 모니터링하고 문제를 해결할 수 있는 다양한 경보 및 보고서를 제공합니다.

경보

Active Directory 오류 및 문제에 대해 다음 경보가 트리거됩니다.

- 구성된 네임서버를 사용할 수 없음
- 가입한 도메인 사용 불가능
- 인증 도메인을 사용할 수 없음
- Active Directory 포리스트를 사용할 수 없음
- AD Connector를 다시 시작해야 함
- AD: ISE 계정 비밀번호 업데이트 실패
- AD: 머신 TGT 새로 고침 실패

보고서

다음 두 보고서를 통해 Active Directory 관련 활동을 모니터링할 수 있습니다.

- RADIUS 인증 보고서: 이 보고서에는 Active Directory 인증 및 권한 부여에 대한 세부 단계가 표시됩니다. **Operations(**운영**)** > **Reports(**보고서**)** > **Endpoints and Users(**엔드포인트 및 사용자**)** > **RADIUS Authentications(RADIUS** 인증**)**에서 이 보고서를 찾을 수 있습니다.
- AD Connector 운영 보고서: AD Connector 운영 보고서는 Cisco ISE 서버 비밀번호 새로 고침, Kerberos 티켓 관리, DNS 쿼리, DC 검색, LDAP 및 RPC 연결 관리 등 AD Connector에서 수행하는 백그라운드 작업 로그를 제공합니다. Active Directory 오류가 발생하는 경우 이 보고서에서 세부 정보를 검토하여 가능한 원인을 파악할 수 있습니다. **Operations(**운영**)** > **Reports(**보고서**)** > **Diagnostics(**진단**)** > **AD Connector Operations(AD Connector** 운영**)**에서 이 보고서를 찾을 수 있습니다.

Active Directory 고급 조정

고급 조정 기능은 시스템에서 매개변수를 더 세부적으로 조정할 수 있도록 Cisco 지원 담당자의 감독하에 지원 작업에 사용되는 노드별 설정을 제공합니다. 이러한 설정은 일반적인 관리 흐름에는 사용되지 않으며 Cisco 지침에 따라서만 사용해야 합니다.

Active Directory ID 검색 속성

Cisco ISE는 SAM, CN 또는 두 속성 모두를 사용하여 사용자를 식별합니다. Cisco ISE, 릴리스 2.2 패치 5 이상 및 2.3 패치 2 이상에서는 sAMAccountName 속성을 기본 속성으로 사용합니다. 이전 릴리스에서는 기본적으로 SAM 및 CN 속성이 모두 검색되었습니다. 이 동작은 CSCvf21978 버그 수정의 일부로 릴리스 2.2 패치 5 이상 및 2.3 패치 2 이상에서 변경되었습니다. 이 릴리스에서는 sAMAccountName 속성만 기본 속성으로 사용됩니다.

사용자 환경에서 필요한 경우 SAM, CN 또는 둘 다를 사용하도록 Cisco ISE를 구성할 수 있습니다. SAM 및 CN이 사용되고 SAMAccountName 속성의 값이 고유하지 않은 경우 Cisco ISE는 CN 속성 값도 비교합니다.

참고 ID 검색 동작은 Cisco ISE 2.4에서 기본적으로 SAM 계정 이름만 검색하도록 변경되었습니다. 이 기본 동작을 수정하려면 "Active Directory ID 검색 속성 구성" 섹션에 설명된 대로 "IdentityLookupField" 플래그의 값을 변경합니다.

Active Directory ID 검색 속성 구성

1. **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **External Identity Sources(**외부 **ID** 소스**)** > **Active Directory**를 선택합니다. **Active Directory** 창에서 **Advanced Tools(**고급 도구**)**를 클릭하고 **Advanced Tuning(**고급 조정**)**을 선택합니다. 다음 세부정보를 입력합니다.
   - **ISE Node(ISE** 노드**)** - Active Directory에 연결 중인 ISE 노드를 선택합니다.
   - **Name(**이름**)** - 변경 중인 레지스트리 키를 입력합니다. Active Directory 검색 속성을 변경하려면 `REGISTRY.Services\lsass\Parameters\Providers\ActiveDirectory\IdentityLookupField`를 입력합니다.
   - **Value(**값**)** - ISE가 사용자를 식별하는 데 사용하는 속성을 입력합니다.
     - *SAM* - 쿼리에서 SAM만 사용하려는 경우(이 옵션이 기본값)
     - *CN* - 쿼리에서 CN만 사용하려는 경우
     - *SAMCN* - 쿼리에서 CN 및 SAM을 사용하려는 경우
   - **Comment(**설명**)** - 변경 사항에 대한 설명(예: Changing the default behavior to SAM and CN)을 입력합니다.
2. **Update Value(**값 업데이트**)**를 클릭하여 레지스트리를 업데이트합니다.

   팝업 창이 나타납니다. 메시지를 읽고 변경 사항을 수락합니다. ISE의 AD Connector 서비스가 다시 시작됩니다.

검색 문자열 예

다음 예에서는 사용자 이름이 *userd2only*라고 가정합니다.

- SAM 검색 문자열 -

```
filter=[(&(|(objectCategory=person)(objectCategory=computer))(|(cn=userd2only)(sAMAccountName=userd2only)))]
```

- SAM 및 CN 검색 문자열 -

```
filter=[(&(|(objectCategory=person)(objectCategory=computer))(sAMAccountName=userd2only))]
```

Active Directory를 사용하여 Cisco ISE를 설정하기 위한 보충 정보

Active Directory를 사용하여 Cisco ISE를 설정하려면 그룹 정책과 머신 인증용 신청자를 구성해야 합니다.

Active Directory에서 그룹 정책 구성

그룹 정책 관리 편집기에 액세스하는 방법에 대한 자세한 내용은 Microsoft Active Directory 설명서를 참고해 주십시오.

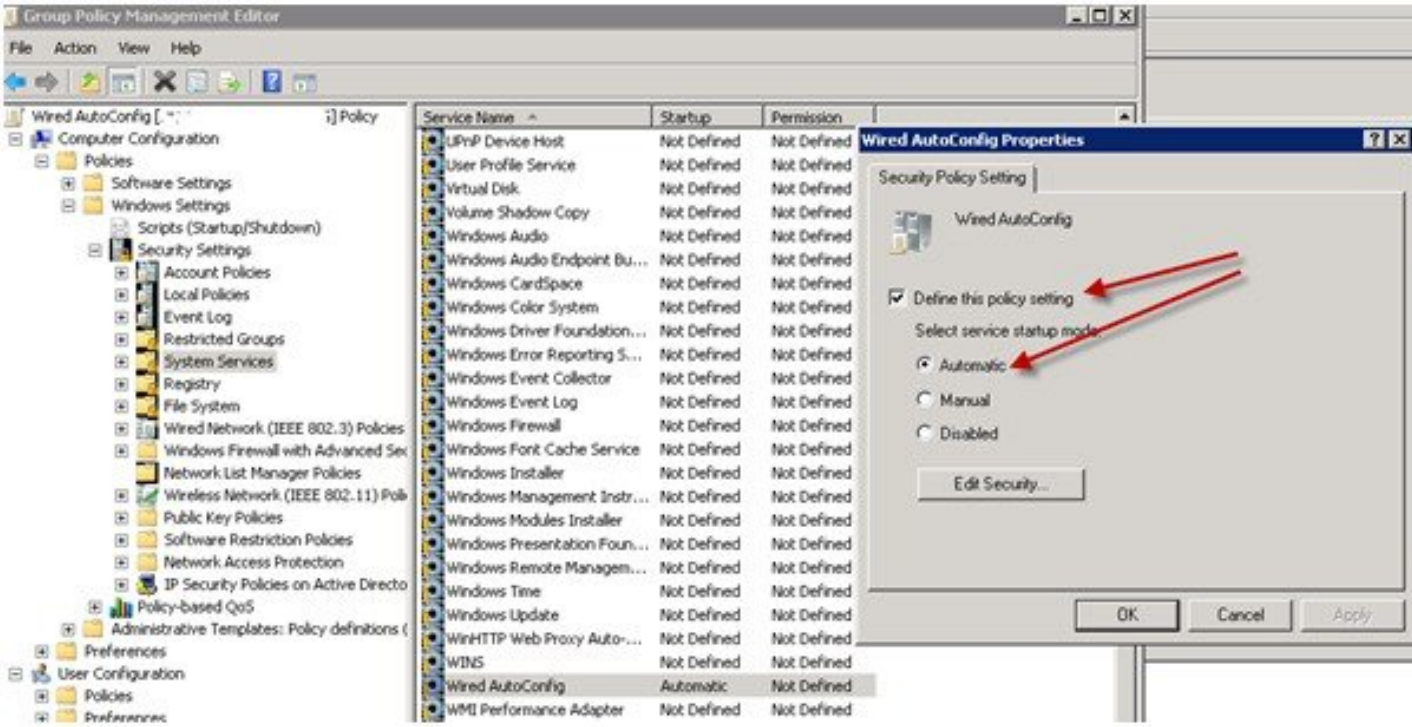
단계 **1** 다음 그림에 나와 있는 것처럼 그룹 정책(Group Policy) 관리 편집기를 엽니다.

그룹 정책 객체(Group Policy Object) 선택

단계 **2** 새 정책을 생성하고 해당 정책을 설명하는 이름을 입력하거나 기존 도메인 정책에 추가합니다.

아래 예에서는 정책 이름으로 Wired Autoconfiguration이 사용되었습니다.

단계 **3** 다음 그림에 나와 있는 것처럼 **Define this policy setting(**이 정책 설정 정의**)** 확인란을 선택하고 서비스 시작 모드로 **Automatic(**자동**)** 라디오 버튼을 클릭합니다.



단계 **4** 원하는 조직 단위 또는 도메인 Active Directory 레벨에 정책을 적용합니다.

Active Directory에 대한 EAP-TLS 머신 인증용 Odyssey 5.X 신청자 구성

Active Directory에 대한 EAP-TLS 머신 인증용으로 Odyssey 5.X 신청자를 사용 중인 경우에는 신청자에서 다음 항목을 구성해야 합니다.

단계 **1** Odyssey Access Client를 시작합니다.

단계 **2** 도구 메뉴에서 **Odyssey Access Client Administrator(Odyssey Access Client** 관리자**)**를 선택합니다.

단계 **3** **Machine Account(**머신 계정**)** 아이콘을 두 번 클릭합니다.

단계 **4** **Machine Account(**머신 계정**)** 창에서 EAP-TLS 인증용 프로파일을 구성해야 합니다.

a) **Configuration(**구성**)** > **Profiles(**프로파일**)**를 선택합니다.
b) EAP-TLS 프로파일의 이름을 입력합니다.
c) Authentication(인증) 탭에서 인증 방법으로 **EAP-TLS**를 선택합니다.
d) Certificate(인증서) 탭에서 **Permit login using my certificate(**내 인증서를 사용한 로그인 허용**)** 확인란을 선택하고 supplicant 머신의 인증서를 선택합니다.
e) **User Info(**사용자 정보**)** 탭에서 **Use machine credentials(**머신 자격 증명 사용**)** 확인란을 선택합니다.

이 옵션을 활성화하면 Odyssey 신청자가 host\<*machine_name*> 형식으로 머신 이름을 전송하며, Active Directory는 해당 요청이 머신에서 수신되는 것으로 식별하여 인증을 수행하기 위한 컴퓨터 객체를 조회합니다. 이 옵션을 비활성화하면 Odyssey 신청자는 host\ 접두사 없이 머신 이름을 전송하며, Active Directory는 사용자 객체를 조회하므로 인증이 실패합니다.

머신 인증용 AnyConnect 에이전트

머신 인증을 위해 AnyConnect 에이전트를 구성하는 경우 다음 중 하나를 수행할 수 있습니다.

- "host/" 접두사가 포함된 기본 머신 호스트 이름을 사용합니다.
- 새 프로파일을 구성합니다. 이 경우 "host/" 접두사와 머신 이름을 차례로 포함해야 합니다.

Easy Connect 및 패시브 ID 서비스 지원을 위한 Active Directory 요건

Easy Connect 및 패시브 ID 서비스는 Active Directory 도메인 컨트롤러에서 생성된 Active Directory 로그인 감사 이벤트를 사용하여 사용자 로그인 정보를 수집합니다. Active Directory 서버를 올바르게 구성해야 ISE 사용자가 서버에 연결하여 사용자 로그인 정보를 가져올 수 있습니다. 다음 섹션에서는 Easy Connect 및 패시브 ID 서비스를 지원하도록 Active Directory 도메인 컨트롤러를 구성하는 방법을 확인할 수 있습니다(Active Directory 측에서의 구성).

Easy Connect 및 패시브 ID 서비스를 지원하도록 Active Directory 도메인 컨트롤러를 구성하려면(Active Directory 측에서의 구성) 다음 단계를 수행합니다.

참고 도메인 전체에서 모든 도메인 컨트롤러를 구성해야 합니다.

1. ISE에서 Active Directory 조인 포인트 및 도메인 컨트롤러를 설정합니다. Active Directory 가입 포인트를 추가하고 해당 가입 포인트에 Cisco ISE 노드 가입, 47 페이지 및 도메인 컨트롤러 추가, 49 페이지를 참조하십시오.
2. 도메인 컨트롤러별 WMI를 구성합니다. 패시브 ID용 WMI 구성, 52 페이지를 참조하십시오.
3. Active Directory에서 다음 단계를 수행합니다.
   - 다음에 대한 Active Directory 설정 구성 패시브 ID 서비스, 69 페이지
   - Windows 감사 정책 설정, 73 페이지
4. (선택 사항) 다음 단계를 수행하여 Active Directory에서 ISE로 수행하는 자동 구성 문제를 해결합니다.
   - Microsoft Active Directory 사용자가 도메인 관리자 그룹에 있을 때의 권한 설정, 74 페이지
   - 도메인 관리자 그룹에 속하지 않은 Microsoft Active Directory 사용자에 대한 권한, 74 페이지
   - 도메인 컨트롤러에서 DCOM을 사용하기 위한 권한, 76 페이지
   - WMI 루트/CIMv2 이름 공간에 대한 액세스 권한 설정, 78 페이지
   - AD 도메인 컨트롤러의 보안 이벤트 로그에 대한 액세스 권한 부여, 79 페이지

다음에 대한 **Active Directory** 설정 구성 패시브 **ID** 서비스

ISE Easy Connect 및 패시브 ID 서비스는 Active Directory 도메인 컨트롤러에서 생성된 Active Directory 로그인 감사 이벤트를 사용하여 사용자 로그인 정보를 수집합니다. ISE는 Active Directory에 연결하여 사용자 로그인 정보를 가져옵니다.

Active Directory 도메인 컨트롤러에서 다음 단계를 수행해야 합니다.

단계 **1** 관련 Microsoft 패치가 Active Directory 도메인 컨트롤러에 설치되어 있는지 확인합니다.

a) Windows Server 2008에는 다음 패치가 필요합니다.

- http://support.microsoft.com/kb/958124

  이 패치는 Microsoft의 WMI에서 메모리 누수를 수정하여, ISE가 도메인 컨트롤러와의 성공적인 연결을 설정할 수 없게 합니다.

- http://support.microsoft.com/kb/973995

이 패치는 때때로 Active Directory 도메인 컨트롤러가 도메인 컨트롤러의 보안 로그에 필요한 사용자 로그인 이벤트를 작성하지 못하도록 하는 Microsoft WMI의 다른 메모리 유출을 수정합니다.

b) Windows Server 2008 R2에는 다음 패치가 필요합니다(SP1이 설치되어 있지 않은 경우).

- http://support.microsoft.com/kb/981314

  이 패치는 때때로 Active Directory 도메인 컨트롤러가 도메인 컨트롤러의 보안 로그에 필요한 사용자 로그인 이벤트를 작성하지 못하도록 하는 Microsoft WMI의 메모리 유출을 수정합니다.

- http://support.microsoft.com/kb/2617858

  이 패치는 Windows Server 2008 R2에서 예기치 않게 발생하는 느린 시작 또는 로그인 프로세스를 수정합니다.

c) Windows 플랫폼의 WMI 관련 문제의 경우 다음 링크에 나열되어 있는 패치가 필요합니다.

- http://support.microsoft.com/kb/2591403

이러한 핫픽스는 WMI 서비스 및 관련 구성 요소의 작동 및 기능과 연관되어 있습니다.

단계 **2** Active Directory가 Windows 보안 로그에 사용자 로그인 이벤트를 기록하는지 확인합니다.

Audit Policy(감사 정책) 설정(Group Policy Management(그룹 정책 관리) 설정의 일부분)의 설정이 Windows 보안 로그에서 필요한 이벤트를 생성하기 위해 정상 로그온을 허용하는지 확인합니다(이는 기본 Windows 설정이지만 이 설정이 올바른지를 명시적으로 확인해야 함).

단계 **3** ISE가 Active Directory에 연결하려면 Active Directory 사용자에게 충분한 권한이 있어야 합니다. 다음 지침에서는 관리 도메인 그룹 사용자 또는 비관리 도메인 그룹 사용자에 대한 권한을 정의하는 방법을 보여줍니다.

- Active Directory 사용자가 도메인 관리자 그룹의 멤버인 경우 필요한 권한
- Active Directory 사용자가 도메인 관리자 그룹의 멤버가 아닌 경우 필요한 권한

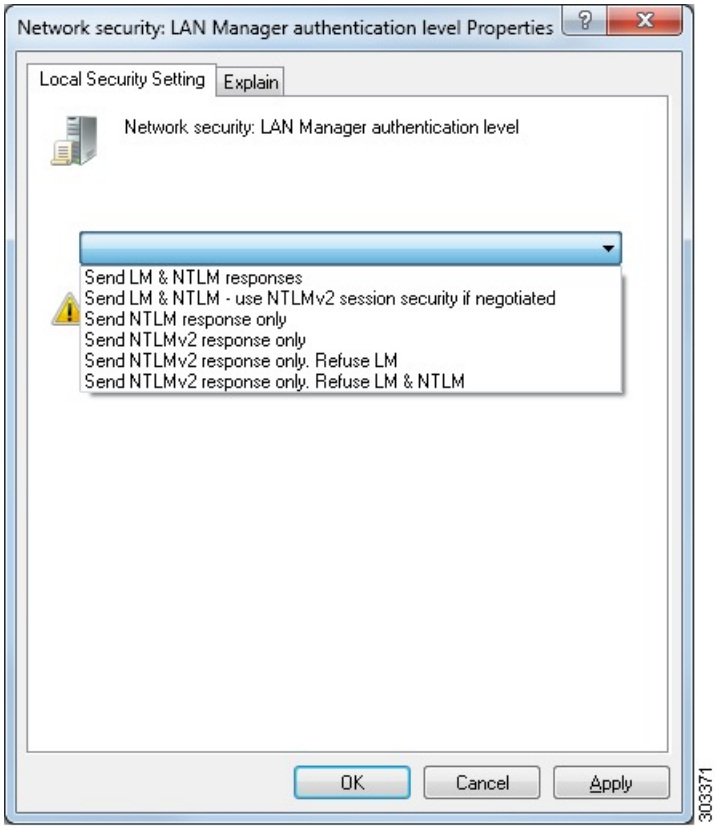
단계 **4** ISE에서 사용하는 Active Directory 사용자는 NTLM(NT LAN Manager) v1 또는 v2로 인증할 수 있습니다. ISE와 Active Directory 도메인 컨트롤러 간에 정상적으로 인증된 연결을 위해 Active Directory NTLM 설정이 ISE NTLM 설정과 일치하는지를 확인해야 합니다. 다음 표에는 모든 Microsoft NTLM 옵션과 지원되는 ISE NTLM 작업이 나와 있습니다. ISE가 NTLMv2로 설정되어 있으면 설명된 6개 옵션이 모두 지원됩니다. ISE가 NTLMv1을 지원하도록 설정되어 있으면 처음 5개 옵션만 지원됩니다.

표 ***15: ISE*** 및 ***AD NTLM*** 버전 설정에 따라 지원되는 인증 유형

ISE NTLM 설정 옵션**/AD(Active Directory) NTLM** 설정 옵션 **NTLMv1** 및 **NTLMv2**	**NTLMv1**	**NTLMv2**
Send LM & NTLM response(LM 및 NTLM 응답 전송) 연결이 허용됨 연결이 허용됨	연결이 허용됨	연결이 허용됨

ISE NTLM 설정 옵션**/AD(Active Directory) NTLM** 설정 옵션 **NTLMv1** 및 **NTLMv2**	**NTLMv1**	**NTLMv2**
Send LM & NTLM - use NTLMv2 session security if negotiated(LM 및 NTLM 전송 - 협상 시 NTLMv2 세션 보안 사용) 연결이 허용됨 연결이 허용됨	연결이 허용됨	연결이 허용됨
Send NTLM response only(NTLM 응답만 전송) 연결이 허용됨 연결이 허용됨	연결이 허용됨	연결이 허용됨
Send NTLMv2 response only(NTLMv2 응답만 전송) 연결이 허용됨 연결이 허용됨	연결이 허용됨	연결이 허용됨
Send NTLMv2 response only. Refuse LM(NTLMv2 응답만 전송하고 LM은 거부) 연결이 허용됨 연결이 허용됨	연결이 허용됨	연결이 허용됨
Send NTLMv2 response only. Refuse LM & NTLM(NTLMv2 응답만 전송하고 LM 및 NTLM은 거부) 연결이 거부됨 연결이 허용됨	연결이 거부됨	연결이 허용됨

그림 ***1: MS NTLM*** 인증 유형 옵션



단계 **5** Active Directory 도메인 컨트롤러에서 `dllhost.exe`에 대한 트래픽을 허용하는 방화벽 규칙을 생성했는지 확인합니다.

방화벽을 끄거나, 특정 IP(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 137: Netbios 이름 확인
- UDP 138: Netbios 데이터그램 서비스
- TCP 139: Netbios 세션 서비스
- TCP 445: SMB

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

모든 방화벽 규칙을 특정 IP(ISE IP)에 할당할 수 있습니다.

Windows 감사 정책 설정

Audit Policy(감사 정책**)(Group Policy Management(**그룹 정책 관리**)** 설정의 일부분)가 정상 로그온을 허용하는지 확인합니다. 이는 AD 도메인 컨트롤러 머신의 Windows 보안 로그에서 필요한 이벤트를 생성하기 위해 필요합니다. 이는 기본 Windows 설정이지만 이 설정이 올바른지 확인해야 합니다.

단계 **1** **Start(**시작**)** > **Programs(**프로그램**)** > **Administrative Tools(**관리 도구**)** > **Group Policy Management(**그룹 정책 관리**)**를 선택합니다.

단계 **2** Domains(도메인) 아래의 관련 도메인으로 이동한 다음 탐색 트리를 펼칩니다.

단계 **3** **Default Domain Controller Policy(**기본 도메인 컨트롤러 정책**)**를 선택하고 마우스 오른쪽 버튼을 클릭한 후에 **Edit(**편집**)**를 선택합니다.

그룹 정책 관리 편집기가 나타납니다.

단계 **4** **Default Domain Controllers Policy(**기본 도메인 컨트롤러 정책**)** > **Computer Configuration(**컴퓨터 컨피그레이션**)** > **Policies(**정책**)** > **Windows Settings(Windows** 설정**)** > **Security Settings(**보안 설정**)**를 선택합니다.

- Windows Server 2003 또는 Windows Server 2008(R2 이외 버전)의 경우 **Local Policies(**로컬 정책**)** > **Audit Policy(**감사 정책**)**를 선택합니다. 두 개의 정책 항목, 즉 **Audit Account Logon Events(**계정 로그온 이벤트 감사**)** 및 **Audit Logon Events(**로그온 이벤트 감사**)**의 경우 해당하는 **Policy Setting(**정책 설정**)**에 **Success** 조건이 직접적 또는 간접적으로 포함되어 있는지 확인합니다. Success 조건을 간접적으로 포함하려면 **Policy Setting(**정책 설정**)**을 **Not Defined(**정의되지 않음**)**로 설정해야 하며, 이는 유효 값이 상위 레벨 도메인에서 상속됨을 나타냅니다. 그리고 해당 상위 레벨 도메인의 **Policy Setting(**정책 설정**)**은 **Success** 조건을 명시적으로 포함하도록 구성해야 합니다.
- Windows Server 2008 R2 및 Windows 2012의 경우 **Advanced Audit Policy Configuration(**고급 감사 정책 컨피그레이션**)** > **Audit Policies(**감사 정책**)** > **Account Logon(**계정 로그온**)**을 선택합니다. 두 개의 정책 항목, 즉 **Audit Kerberos Authentication Service(Kerberos** 인증 서비스 감사**)** 및 **Audit Kerberos Service Ticket Operations(Kerberos** 서비스 티켓 작업 감사**)**의 경우 위에서 설명한 대로 해당하는 Policy Setting(정책 설정)에 Success 조건이 직접적 또는 간접적으로 포함되어 있는지 확인합니다.

  참고 Cisco ISE는 Active Directory 도메인 컨트롤러 컨피그레이션에서 이 암호화 유형을 비활성화하지 않는 한 Active Directory와 통신하면서 Kerberos 프로토콜에서 RC4 암호를 사용합니다. Active Directory에서 **Network Security: Configure Encryption Types Allowed for Kerberos(**네트워크 보안**: Kerberos** 에 허용되는 암호화 유형 구성**)** 옵션을 사용하여 Kerberos 프로토콜에 대해 허용되는 암호화 유형을 구성할 수 있습니다.

단계 **5** 감사 정책 항목 설정이 변경된 경우에는 `gpupdate /force`를 실행하여 새 설정을 강제로 적용해야 합니다.

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, 76 페이지
- WMI 루트/CIMv2 이름 공간에 대한 액세스 권한 설정, 78 페이지

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 ***2:*** 액세스 권한에 대한 로컬 및 ***Remote Access***

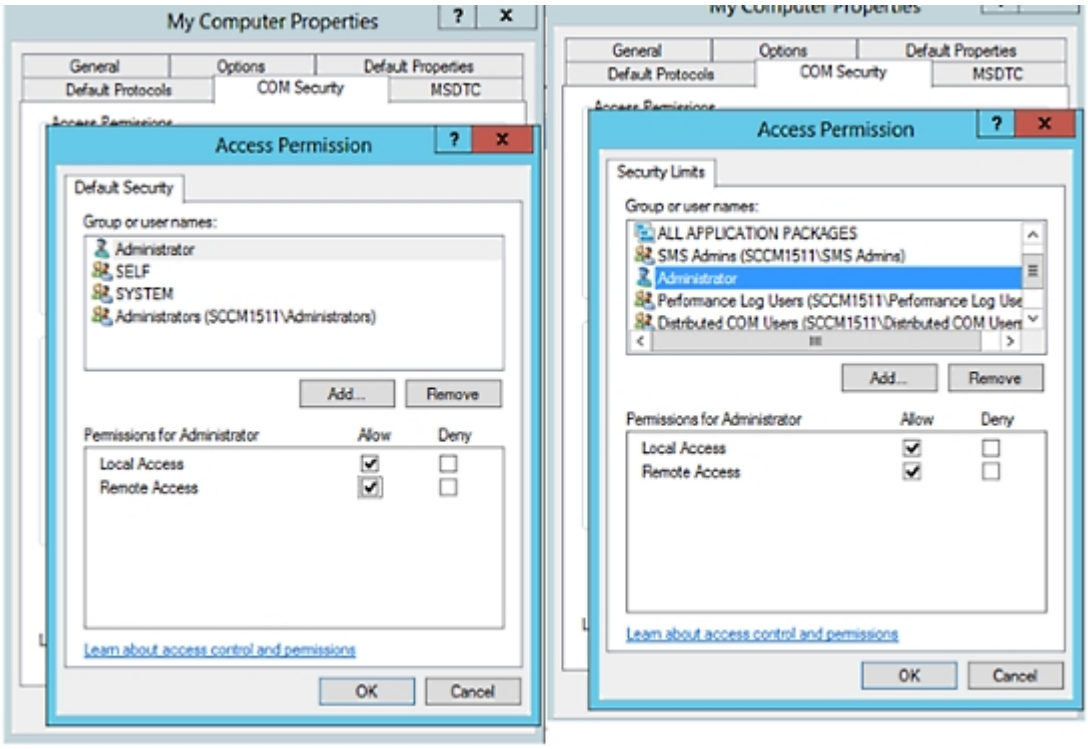
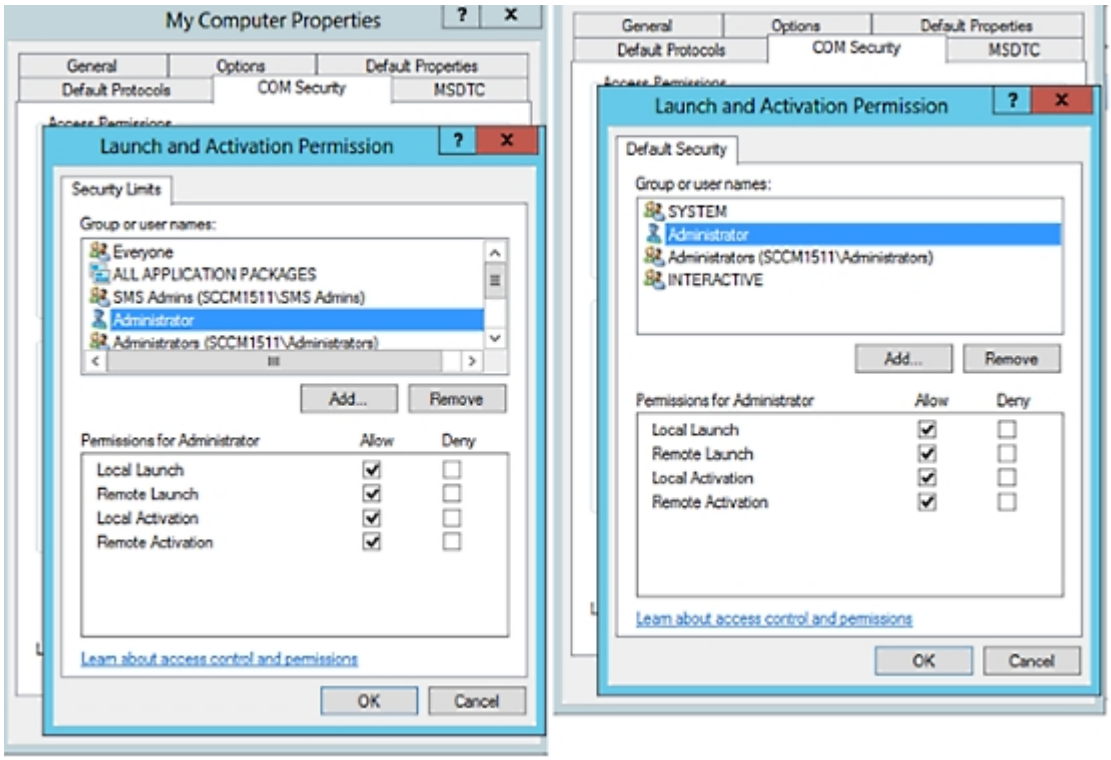


그림 *3:* 실행 및 활성화 권한에 대한 로컬 및 ***Remote Access***



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.

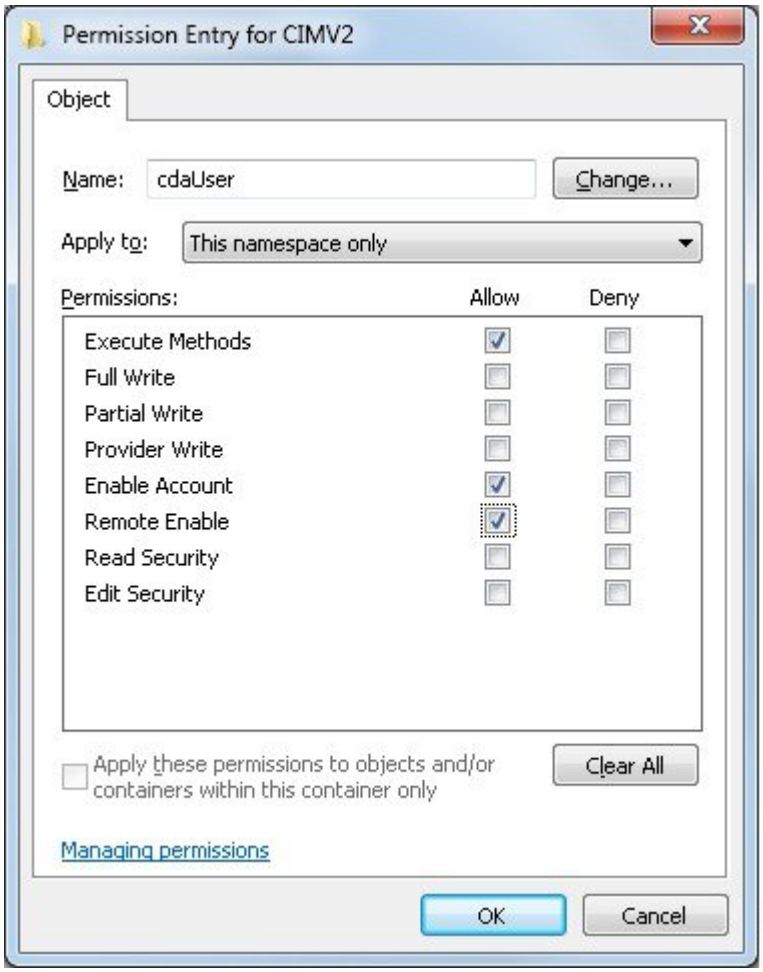
단계 **2** **WMI Control(WMI** 컨트롤**)**을 마우스 오른쪽 버튼으로 클릭하고 **Properties(**속성**)**를 클릭합니다.

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 *4: WMI Root\CIMv2* 이름 공간에 필요한 권한



AD 도메인 컨트롤러의 보안 이벤트 로그에 대한 액세스 권한 부여

Windows 2008 이상에서는 Event Log Readers라는 그룹에 ISE ID 매핑 사용자를 추가하여 AD 도메인 컨트롤러 로그에 대한 액세스 권한을 부여할 수 있습니다.

모든 이전 버전 Windows에서는 아래에 나와 있는 것처럼 레지스트리 키를 편집해야 합니다.

단계 **1** 보안 이벤트 로그에 대한 액세스 권한을 위임하려면 계정의 SID를 찾습니다.

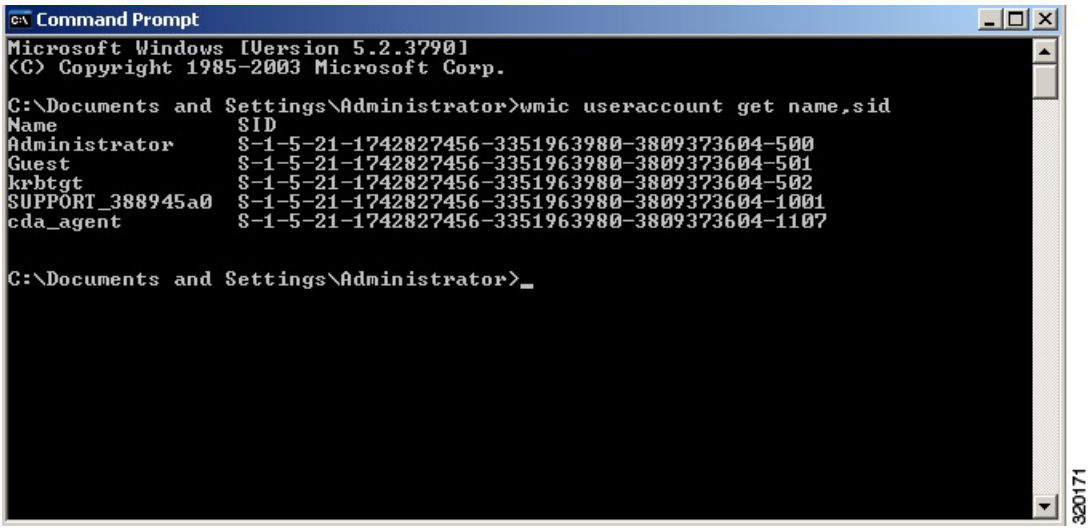
단계 **2** 명령줄에서 다음 명령을 사용하여 모든 SID 계정을 나열합니다. 이 명령은 아래 다이어그램에도 나와 있습니다.

```
wmic useraccount get name,sid
```

특정 사용자 이름 및 도메인의 경우 다음 명령을 사용할 수도 있습니다.

```
wmic useraccount where name="iseUser" get domain,name,sid
```

그림 *5:* 모든 ***SID*** 계정 나열



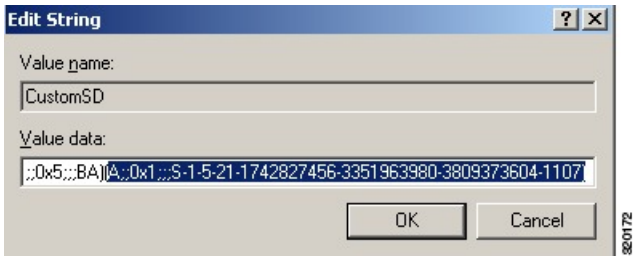
단계 **3** SID를 찾고 레지스트리 편집기를 연 후에 다음 위치로 이동합니다.

`HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/Services/Eventlog`

단계 **4** **Security(**보안**)**를 클릭하고 **CustomSD**를 두 번 클릭합니다.

예를 들어 ise_agent 계정 `(SID - S-1-5-21-1742827456-3351963980-3809373604-1107)`에 읽기 권한을 허용하려면 `(A;;0x1;;;S-1-5-21-1742827456-3351963980-3809373604-1107)`을 입력합니다.

그림 *6:* ***CustomSD*** 문자열 편집



단계 **5** 도메인 컨트롤러에서 WMI 서비스를 다시 시작합니다. 다음과 같이 두 가지 방법으로 WMI 서비스를 다시 시작할 수 있습니다.

a) CLI에서 다음 명령을 실행합니다.

net stop winmgmt

net start winmgmt

b) `Services.msc`를 실행합니다. 그러면 Windows 서비스 관리 툴이 열립니다. Windows 서비스 관리 윈도우에서 **Windows Management Instrumentation** 서비스를 찾아 마우스 오른쪽 버튼으로 클릭한 후에 **Restart(**다시 시작**)**를 선택합니다.

Easy Connect

Easy Connect를 사용하면 사용자를 유선 엔드포인트에서 네트워크로 안전하게 연결한 다음 Cisco ISE가 아닌 Active Directory 도메인 컨트롤러를 통해 사용자를 인증하여 모니터링할 수 있습니다. Easy Connect를 통해 Cisco ISE는 Active Directory 도메인 컨트롤러에서 사용자 인증 정보를 수집합니다. Easy Connect는 MS WMI 인터페이스를 사용하여 Windows 시스템(Active Directory)에 연결하며 Windows 이벤트 메시징에서 로그를 쿼리하므로 현재 Windows가 설치된 엔드포인트만 지원합니다. Easy Connect는 802.1X보다 훨씬 구성하기 쉬운 MAB를 사용하는 유선 연결을 지원합니다. 802.1X와는 달리 Easy Connect 및 MAB를 사용하는 경우:

- 신청자를 구성할 필요가 없습니다.
- PKI를 구성할 필요가 없습니다.
- 외부 서버(AD)가 사용자를 인증하고 나면 ISE에서 CoA를 발급합니다.

Easy Connect는 다음과 같은 작동 모드를 지원합니다.

- 시행 모드: ISE가 사용자 자격 증명을 기준으로 하는 시행을 위해 네트워크 디바이스에 권한 부여 정책을 실제로 다운로드합니다.
- 가시성 모드: Cisco ISE가 NAD 디바이스 센서에서 수신한 세션 병합 및 계정 관리 정보를 게시하여 해당 정보를 pxGrid로 전송합니다.

두 가지 경우 모두, AD(Active Directory)에서 인증된 사용자는 Cisco ISE 라이브 세션 보기에 표시되므로 서드파티 애플리케이션에서 Cisco pxGrid 인터페이스를 사용하여 세션 디렉토리에서 해당 사용자를 쿼리할 수 있습니다. 알려진 정보는 사용자 이름, IP 주소, AD DC 호스트 이름 및 AD DC NetBios 이름입니다. pxGrid에 대한 자세한 내용은 Cisco pxGrid 노드를 참고하십시오.

Easy Connect를 설정하면 이름 또는 IP 주소를 기준으로 특정 사용자를 필터링할 수 있습니다. 예를 들어 엔드포인트를 이용해 일반 관리자를 지원하고자 엔드포인트에 로그인한 IT 서비스 관리자가 있다면, 관리자 활동을 필터링하여 Live Sessions(라이브 세션)에는 표시하지 않고 관련 엔드포인트의 일반 사용자에게만 표시되게 할 수 있습니다. 수동 ID 서비스를 필터링하는 방법은 패시브 ID 서비스 필터링, 131 페이지 항목을 참조하십시오.

Easy Connect 제한

- MAB(MAC Authentication Bypass)는 Easy Connect를 지원합니다. MAB와 802.1X를 둘 다 동일한 포트에 구성할 수는 있지만 각 서비스에 대해 서로 다른 ISE 정책을 사용해야 합니다.
- 현재는 MAB 연결만 지원됩니다. 연결에 대해 고유한 인증 정책이 필요하지 않습니다. 권한 부여 정책에 정의된 Easy Connect 조건에 의해 연결에 권한이 부여되며 사용 권한이 부여되기 때문입니다.
- Easy Connect는 고가용성 모드에서 지원됩니다. 수동 ID로 여러 노드를 정의하고 활성화할 수 있습니다. 그러면 ISE가 PSN 하나를 자동으로 활성화하며 나머지 노드는 스탠바이 상태로 유지됩니다.
- Cisco NAD(Network Access Device)만 지원됩니다.

- IPv6은 지원되지 않습니다.
- 무선 연결은 현재 지원되지 않습니다.
- Kerberos 인증 이벤트만 추적되며, 따라서 Easy Connect는 사용자 인증만 활성화하며 머신 인증은 지원하지 않습니다.

Easy Connect를 사용하려면 ISE에서 컨피그레이션을 수행해야 합니다. 또한 Active Directory 도메인 서버에도 Microsoft에서 발급한 지침에 따라 올바른 패치와 컨피그레이션을 적용해야 합니다. Cisco ISE용 Active Directory 도메인 컨트롤러 구성에 대한 자세한 내용은 다음 항목을 참고하십시오. Easy Connect 및 패시브 ID 서비스 지원을 위한 Active Directory 요건, 68 페이지

Easy Connect 시행 모드

Easy Connect를 사용하면 사용자는 MAB(MAC Address Bypass) 프로토콜을 사용하고 인증을 위해 AD(Active Directory)에 액세스하여 Windows 운영체제가 설치된 유선 엔드포인트(일반적으로 PC)에서 보안 네트워크에 로그온할 수 있습니다. Easy Connect는 인증된 사용자에 대한 정보를 위해 Active Directory 서버에서 WMI(Windows Management Instrumentation) 이벤트를 수신 대기합니다. AD가 사용자를 인증하면 도메인 컨트롤러는 사용자에 대해 할당된 사용자 이름과 IP 주소를 포함하는 이벤트 로그를 생성합니다. Cisco ISE는 AD에서 로그인 알림을 수신한 다음 RADIUS CoA(Change of Authorization)를 발급합니다.

참고 RADIUS 서버 유형이 통화 확인으로 설정되어 있는 경우 MAC 주소 조회는 MAB 요청에 대해 수행되지 않습니다. 따라서 요청에 대해 액세스 수락이 반환됩니다. 이 응답이 기본 구성입니다.

Easy Connect 시행 모드 프로세스 플로우

Easy Connect 시행 모드 프로세스는 다음과 같습니다.

1. 사용자가 유선 엔드포인트(예: PC 등)에서 NAD에 연결합니다.
2. MAB용으로 구성된 NAD가 Cisco ISE에 액세스 요청을 보냅니다. Cisco ISE는 사용자 구성을 기준으로 하는 액세스 권한으로 응답하여 사용자의 AD 액세스를 허용합니다. 구성은 최소한 DNS, DHCP 및 AD 액세스를 허용해야 합니다.
3. 사용자가 도메인에 로그인하면 보안 감사 이벤트가 Cisco ISE로 전송됩니다.
4. ISE가 RADIUS의 MAC 주소, IP 주소 및 도메인 이름을 수집하며 보안 감사 이벤트에서 사용자에 대한 계정 관리 정보(로그인 정보)도 수집합니다.
5. 모든 데이터가 수집되어 세션 디렉터리에 병합되면 Cisco ISE는 NAD에 CoA를 발급하며(정책 서비스 노드에서 관리되는 적절한 정책 기준), 해당 정책을 기준으로 NAD가 사용자에게 네트워크 액세스 권한을 제공합니다.

그림 ***7: Easy Connect*** 시행 모드 기본 플로우

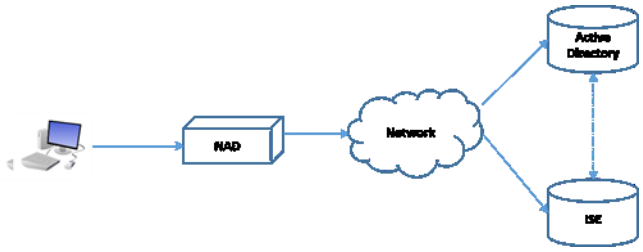
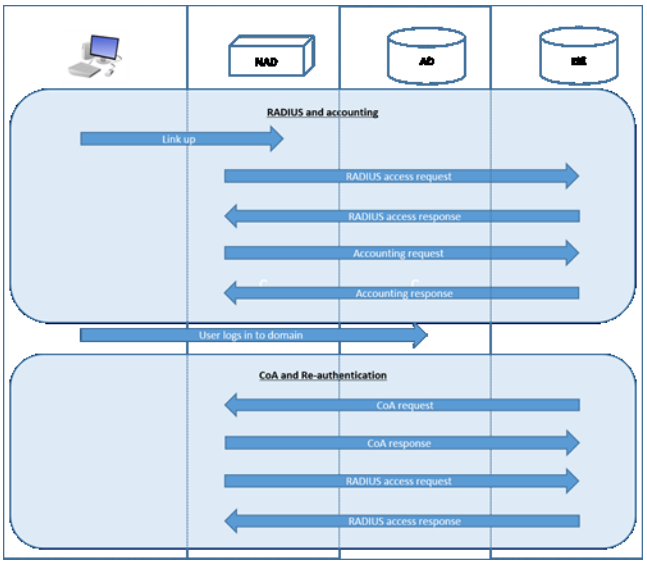


그림 ***8: Easy Connect*** 시행 모드 상세 플로우

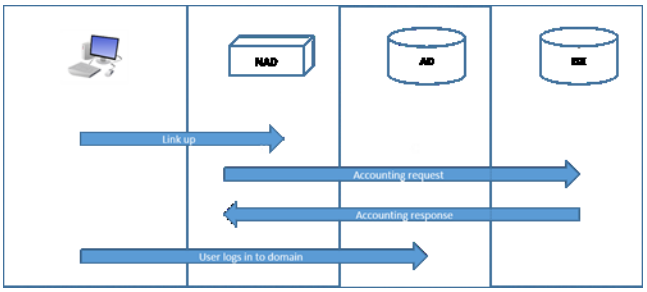


시행 모드 구성에 대한 자세한 내용은 Easy Connect 시행 모드 구성, 84 페이지를 참고하십시오.

Easy Connect 가시성 모드

가시성 모드에서는 Cisco ISE가 RADIUS(NAD의 디바이스 센서 기능의 일부분)에서 계정 관리 정보만을 모니터링하며 권한 부여는 수행하지 않습니다. Easy Connect는 RADIUS 계정 관리 및 WMI 이벤트를 수신 대기하며 해당 정보를 로그 및 보고서에 게시합니다(pxGrid에는 선택적으로 게시). pxGrid가 설정되어 있는 경우 Active Directory를 사용하는 사용자 로그인 중에 RADIUS 계정 관리 시작 및 세션 종료가 모두 pxGrid에 게시됩니다.

그림 ***9: Easy Connect*** 가시성 모드 플로우



Easy Connect 가시성 모드 구성에 대한 자세한 내용은 EasyConnect 가시성 모드 구성, 85 페이지를 참고하십시오.

Easy Connect 시행 모드 구성

시작하기 전에

- 최고의 성능을 위해서는 WMI 이벤트 수신 전용 PSN을 구축합니다.
- AD 로그인 이벤트를 수신하는 WMI 노드에 대해 Active Directory 도메인 컨트롤러 목록을 생성합니다.
- Cisco ISE가 Active Directory에서 사용자 그룹을 가져오려면 가입해야 하는 Microsoft 도메인을 확인합니다.
- 권한 부여 정책에서 참조로 사용되는 Active Directory 그룹을 확인합니다.
- pxGrid를 사용하여 네트워크 디바이스의 세션 데이터를 다른 pxGrid가 활성화된 시스템과 공유하는 경우에는 구축에서 pxGrid 페르소나를 정의합니다. pxGrid에 대한 자세한 내용은 다음을 참고하십시오. Cisco pxGrid 노드
- MAB가 정상적으로 수행되고 나면 NAD는 제한적 액세스 프로파일을 제공해야 합니다. 그러면 개요의 설명과 같이 해당 포트의 사용자가 Active Directory 서버에 액세스할 수 있습니다.

참고 여러 노드에서 Passive Identity Service를 활성화할 수는 있지만 EasyConnect는 한 번에 한 노드에서만 작동할 수 있습니다. 여러 노드에 대해 서비스를 활성화하면 ISE는 활성화된 EasyConnect 세션에 사용할 노드를 자동으로 결정합니다.

단계 **1** **Administration(**관리**)** > **System(**시스템**)** > **Deployment(**구축**)**를 선택한 후 노드를 열고 **General Settings(**일반 설정**)** 아래에서 **Enable Passive Identity Service(**패시브 **ID** 서비스 활성화**)**를 활성화합니다.

단계 **2** Easy Connect에서 사용할 Active Directory 조인 포인트와 도메인 컨트롤러를 구성합니다. 자세한 내용은 Easy Connect 및 패시브 ID 서비스 지원을 위한 Active Directory 요건, 68 페이지를 참고하십시오.

단계 **3** **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **External Identity Sources(**외부 **ID** 소스**)** > **Active Directory**를 선택합니다. **Groups(**그룹**)** 탭을 클릭하고 인증 정책에 사용할 Active Directory 그룹을 추가합니다.
도메인 컨트롤러에 대해 매핑하는 Active Directory 그룹은 PassiveID 사전에서 동적으로 업데이트되며, 정책 조건 규칙을 설정할 때 이러한 그룹을 사용할 수 있습니다.

단계 **4** 참고 EasyConnect 프로세스가 올바르게 실행하고 ISE가 CoA를 발급하도록 활성화하려면 EasyConnect 권한 부여에 사용되는 모든 프로파일에 대해 **Passive Identity Tracking(**수동 **ID** 추적**)**을 활성화해야 합니다.

Policy(정책**)** > **Policy Elements(**정책 요소**)** > **Results(**결과**)** > **Authorization(**권한 부여**)** > **Authorization Profiles(**권한 부여 프로파일**)**를 선택합니다. EasyConnect에서 사용할 프로파일의 경우 해당 프로파일을 열고 **Passive Identify Tracking(**수동 **ID** 추적**)**을 활성화합니다.

단계 **5** 정책 규칙을 생성합니다. 이렇게 하려면 **Policy(**정책**)** > **Policy Elements(**정책 요소**)** > **Conditions(**조건**)** > **Authorization(**권한 부여**)** > **Simple Conditions(**단순 조건**)**를 선택하고 EasyConnect용 규칙을 생성합니다. **Add(**추가**)**를 클릭하고 조건을 정의합니다.

a) 이름과 설명을 입력합니다.

b) **Attribute(**속성**)**에서 PassiveID 사전으로 이동한 다음 PassiveID_Groups를 선택하여 도메인 컨트롤러 그룹용 조건을 생성하거나, PassiveID_user를 선택하여 개별 사용자용 조건을 생성합니다.

c) 올바른 작업을 입력합니다.

d) 정책에 포함할 사용자 이름 또는 그룹 이름을 입력합니다.

단계 **6** **Submit(**제출**)**을 클릭합니다.

EasyConnect 가시성 모드 구성

시작하기 전에

- 최고의 성능을 위해서는 WMI 이벤트 수신 전용 PSN을 구축합니다.
- AD 로그인 이벤트를 수신하는 WMI 노드에 대해 Active Directory 도메인 컨트롤러 목록을 생성합니다.
- Cisco ISE가 Active Directory에서 사용자 그룹을 가져오려면 가입해야 하는 Microsoft 도메인을 확인합니다.
- pxGrid를 사용하여 네트워크 디바이스의 세션 데이터를 다른 pxGrid가 활성화된 시스템과 공유하는 경우에는 구축에서 pxGrid 페르소나를 정의합니다. pxGrid에 대한 자세한 내용은 다음을 참고하십시오. Cisco pxGrid 노드

단계 **1** **Administration(**관리**)** > **System(**시스템**)** > **Deployment(**구축**)**를 선택한 후 노드를 열고 **General Settings(**일반 설정**)** 아래에서 **Enable Passive Identity Service(**패시브 **ID** 서비스 활성화**)**를 활성화합니다.

단계 **2** Easy Connect에서 사용할 Active Directory 조인 포인트와 도메인 컨트롤러를 구성합니다. 자세한 내용은 Easy Connect 및 패시브 ID 서비스 지원을 위한 Active Directory 요건, 68 페이지를 참고하십시오.

PassiveID 작업 센터

Passive Identity Connector(PassiveID 작업 센터)는 중앙 집중식 원스톱 설치 및 구현을 제공하기 때문에, 사용자는 네트워크를 쉽고 간단하게 구성해 사용자 ID 정보를 받고 Cisco FMC(Firepower Management Center)나 Stealthwatch 같은 다양한 보안 제품 가입자와 공유할 수 있습니다. 수동 식별의 전체 브로커로서 PassiveID 작업 센터는 AD DC(Active Directory Domain Controller) 같은 다양한 제공자 소스로부터 사용자 ID를 수집하고, 사용자 로그인 정보를 사용 중인 관련 IP 주소에 매핑한 다음 매핑 정보를 사용자가 구성한 가입자 보안 제품과 공유합니다.

Passive Identity(패시브 ID)란?

Cisco Identity Services Engine(ISE)에서 제공하는 표준 흐름으로, AAA(인증, 권한 부여 및 계정 관리) 서버를 제공하며 802.1X나 Web Authentication(웹 인증) 같은 기술을 활용하고, 사용자 또는 엔드포인트와 직접 통신해 네트워크 액세를 요청한 다음 관련 로그인 자격 증명을 이용해 ID를 확인하고 활성 인증합니다.

패시브 ID 서비스는 사용자를 직접 인증하는 대신 서비스 제공자로 확인된 (Active Directory 같은) 외부 인증 서버에서 사용자 ID와 IP 주소를 수집한 다음 이 정보를 가입자와 공유합니다. PassiveID 작업 센터는 먼저 서비스 제공자로부터 (대부분 사용자 로그인 및 비밀번호를 바탕으로) 사용자 ID 정보를 수신한 다음 필요한 확인 작업과 서비스를 수행하여 사용자 ID를 관련 IP 주소와 매치함으로써 인증된 IP 주소를 가입자에게 전달합니다.

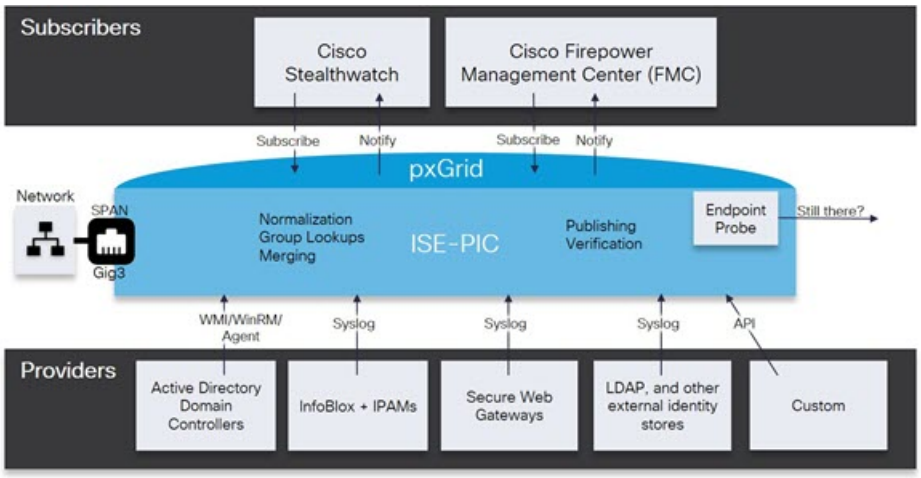
Passive Identity Connector(PassiveID 작업 센터) 플로우

PassiveID 작업 센터의 흐름은 다음과 같습니다.

1. 서비스 제공자가 사용자 또는 엔드포인트의 인증을 수행합니다.
2. 서비스 제공자가 인증된 사용자 정보를 Cisco ISE에 전송합니다.
3. Cisco ISE는 사용자 정보를 정규화하고 관련 조회와 병합 및 구문 분석을 수행하며 IP 주소에 매핑하고, 매핑한 세부정보를 pxGrid에 게시합니다.
4. pxGrid 가입자는 매핑된 사용자 세부정보를 수신합니다.

다음 다이어그램에서는 Cisco ISE에서 제공되는 개괄적인 플로우에 대해 설명합니다.

그림 *10:* 고수준 흐름



초기 설정 및 컨피그레이션

Cisco PassiveID 작업 센터를 빠르게 사용하려면 다음 흐름을 따르십시오.

1. DNS 서버를 올바르게 구성했는지 확인합니다(Cisco ISE에서의 클라이언트 머신에 대한 역방향 조회 구성 포함). 자세한 내용은 DNS 서버, 46 페이지를 참고하십시오.

2. 패시브 ID 서비스에 사용할 전용 정책 서버(PSN)에서 패시브 ID 및 pxGrid 서비스를 활성화합니다. **Administration(관리)** > **System(시스템)** > **Deployment(구축)**를 선택한 후 노드를 열고 **General Settings(일반 설정)** 아래에서 **Enable Passive Identity Service(패시브 ID 서비스 활성화)** 및 **pxGrid**를 활성화합니다.
3. NTP 서버의 시계 설정을 동기화합니다.
4. ISE Passive Identity(ISE 패시브 ID) 설정을 사용하여 초기 서비스 제공자를 구성합니다. 자세한 내용은 다음을 참조하십시오. PassiveID(패시브 ID) 설정 시작하기 , 89 페이지
5. 단일 또는 다중 가입자를 구성합니다. 자세한 내용은 다음을 참조하십시오. 가입자, 134 페이지

최초 서비스 제공자와 가입자를 설정하면 추가 서비스 제공자를 쉽게 생성하고(추가 패시브 ID 서비스 제공자, 94 페이지 참조) PassiveID 작업 센터:에서 다른 서비스 제공자의 패시브 ID를 관리할 수 있습니다(PassiveID Work Center(패시브 ID 작업 센터)에서의 모니터링 및 문제 해결 PassiveID 작업 센터, 138 페이지 참조).

- RADIUS 라이브 세션
- Cisco ISE 경보
- Cisco ISE 보고서
- 들어오는 트래픽을 검증하는 TCP 덤프 유틸리티

PassiveID 작업 센터 Dashboard(대시보드)

Cisco PassiveID 작업 센터 대시보드에는 상관관계가 분석되고 통합된 요약 및 통계 데이터가 표시되는데, 이는 효과적인 모니터링 및 문제 해결을 위해서는 필수적이며 실시간으로 업데이트됩니다. dashlet에서는 별도의 설명이 없는 한 지난 24시간 동안의 활동을 표시합니다. 대시보드에 액세스하려면 **Work Centers(작업 센터)** > **PassiveID(패시브 ID)**를 선택한 다음 왼쪽 패널에서 **Dashboard(대시보드)**를 선택합니다. PAN(Primary Administration Node)에서만 Cisco PassiveID 작업 센터 대시보드를 볼 수 있습니다.

- **Main(기본)** 보기에는 선형 메트릭 대시보드, 차트 dashlet 및 목록 dashlet이 있습니다. PassiveID 작업 센터에서는 dashlet을 구성할 수 없습니다. 제공되는 dashlet은 다음과 같습니다.
  - **Passive Identity Metrics(패시브 ID 메트릭)**: 현재 추적 중인 총 고유 라이브 세션 수, 시스템에 구성된 총 ID 제공자 수, ID 데이터를 능동적으로 전달하는 총 에이전트 수, 현재 구성된 총 가입자 수를 표시합니다.
  - **Provider(제공자)**: 제공자는 사용자 ID 정보를 PassiveID 작업 센터에 제공합니다. 제공자 소스에서 정보를 수신하는 데 사용할 ISE 프로브(지정된 소스에서 데이터를 수집하는 메커니즘)를 구성합니다. 예를 들어 AD(Active Directory) 프로브와 에이전트 프로브는 각기 다른 기술을 사용하여 ISE-PIC가 AD에서 데이터를 수집하는 데 도움을 주는 한편, 시스템 로그 프로브는 시스템 로그 메시지를 읽는 구문 분석기에서 데이터를 수집합니다.
  - **Subscribers(가입자)**: 가입자는 사용자 ID 정보를 검색하기 위해 ISE에 연결합니다.

- **OS Types(OS** 유형**)**: 표시할 수 있는 OS 유형은 Windows뿐입니다. Windows 유형은 Windows 버전별로 표시됩니다. 제공자는 OS 유형을 보고하지 않지만 ISE는 Active Directory를 쿼리하여 해당 정보를 가져올 수 있습니다. dashlet에는 최대 1,000개의 항목이 표시됩니다.
- **Alarms(**경보**)**: 사용자 ID 관련 경보입니다.

프로브 및 제공자로서의 **Active Directory**

Active Directory(AD)는 사용자 이름, IP 주소 및 도메인 이름 같은 사용자 ID 정보를 수신할 수 있는 대단히 안전하고 정확한 소스입니다.

AD 프로브인 패시브 ID 서비스는 WMI 기술을 이용해 AD에서 사용자 ID 정보를 수신하지만, 다른 프로브는 다른 기술 과 방법을 이용해 AD를 사용자 ID 제공자로 사용합니다. ISE에서 제공하는 다른 프로브 및 제공자 유형에 관한 자세한 내용은 추가 패시브 ID 서비스 제공자, 94 페이지 항목을 참조하십시오.

Active Directory 프로브를 구성하면 (마찬가지로 Active Directory를 소스로 사용하는) 이러한 다른 프로브를 빠르게 구성하고 활성화할 수 있습니다.

- Active Directory 에이전트, 97 페이지

참고 Active Directory 에이전트는 Windows Server 2008 이상에서만 지원됩니다.

- SPAN, 107 페이지
- 엔드포인트 프로브, 131 페이지

또한 사용자 정보를 수집할 때 AD 사용자 그룹을 사용할 수 있도록 Active Directory 프로브를 구성합니다. AD 사용자 그룹을 AD, 에이전트, SPAN 및 시스템 로그 프로브에 사용할 수 있습니다. AD 그룹에 관한 자세한 내용은 Active Directory 사용자 그룹 구성, 54 페이지 항목을 참조하십시오.

Active Directory(WMI) 프로브 설정

패시브 ID 서비스에 대해 Active Directory와 WMI를 구성하려면 Passive ID Work Center Wizard(패시브 ID 작업 센터 마법사)(PassiveID(패시브 ID) 설정 시작하기 , 89 페이지 참조)를 사용하거나 아래 단계를 따르십시오.

1. Active Directory 도메인을 구성합니다. Active Directory 가입 포인트를 추가하고 해당 가입 포인트에 Cisco ISE 노드 가입, 47 페이지를 참조하십시오.
2. AD 로그인 이벤트를 수신하는 WMI 구성 노드(또는 노드 모음)에 대한 Active Directory 도메인 컨트롤러 목록을 생성합니다. 도메인 컨트롤러 추가, 49 페이지를 참조하십시오.
3. ISE와 통합할 수 있도록 Active Directory를 구성합니다. 패시브 ID용 WMI 구성, 52 페이지를 참조하십시오.
4. (선택 사항) Active Directory 제공자 관리, 91 페이지.

자세한 내용은 Easy Connect 및 패시브 ID 서비스 지원을 위한 Active Directory 요건, 68 페이지를 참고하십시오.

PassiveID(패시브 ID) 설정 시작하기

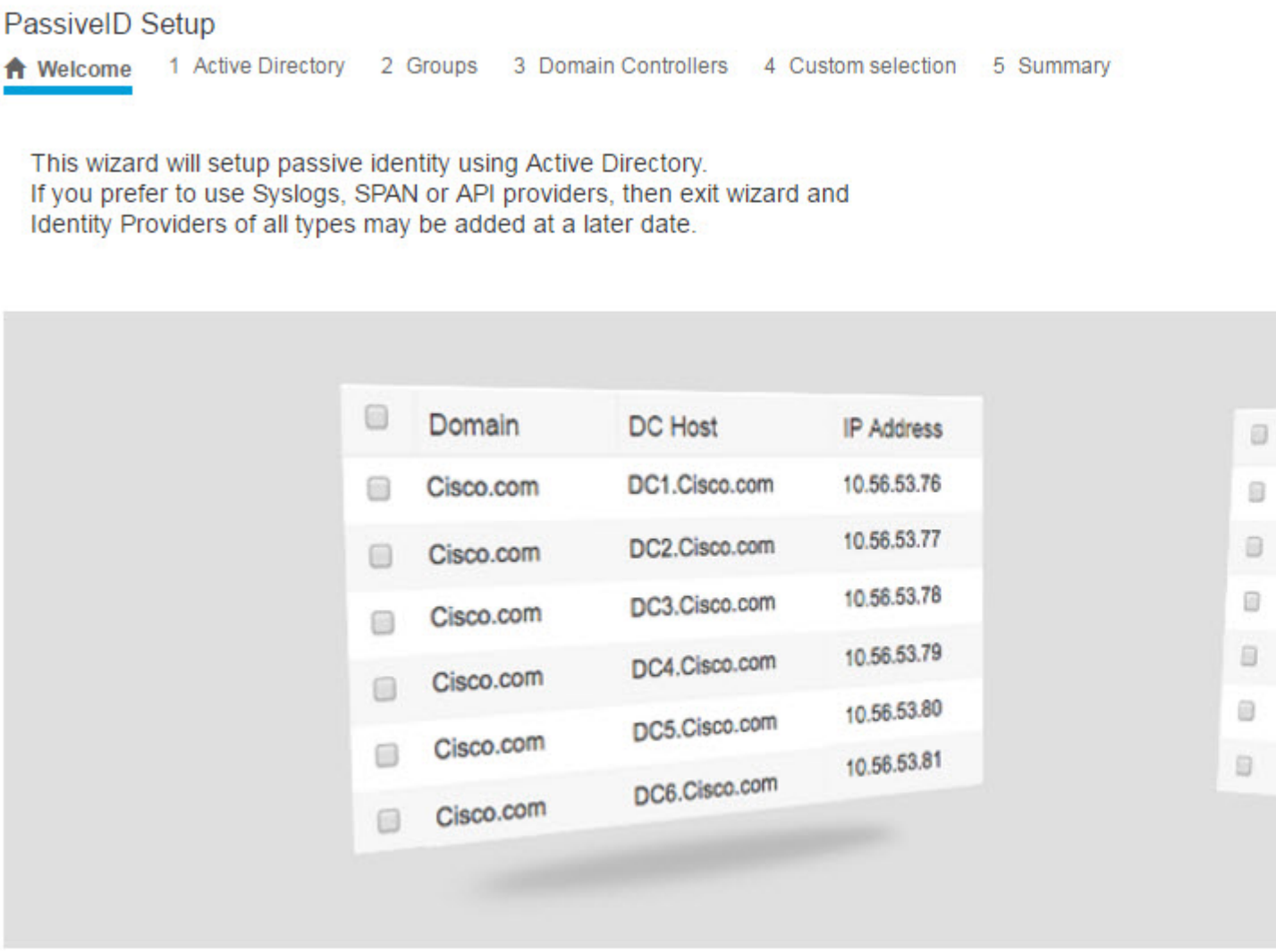
ISE-PIC Active Directory를 첫 번째 사용자 ID 제공자로 쉽고 빠르게 구성하여 Active Directory에서 사용자 ID를 수신할 수 있는 마법사를 제공합니다. ISE-PIC용으로 Active Directory를 구성하면, 나중에 다른 제공자 유형도 쉽게 구성할 수 있습니다. Active Directory를 구성한 후에는 가입자(isco FMC(Firepower Management Center) 또는 Stealthwatch 등)를 구성해야 사용자 데이터를 수신할 클라이언트를 정의할 수 있습니다. 가입자에 관한 자세한 내용은 가입자, 134 페이지 항목을 참조하십시오.

시작하기 전에

- Microsoft Active Directory 서버가 네트워크 주소 변환기 뒤에 배치되지 않고 NAT(Network Address Translation) 주소를 갖지 않는지 확인합니다.
- 가입 작업에 사용되는 Microsoft Active Directory 계정이 유효하며 Change Password on Next Login(다음 로그인 시 비밀번호 변경)을 사용하여 구성되지 않았는지 확인합니다.
- ISE에 슈퍼 관리자 또는 시스템 관리자 권한이 있어야 합니다.
- 패시브 ID 서비스에 사용할 전용 정책 서버(PSN)에서 패시브 ID 및 pxGrid 서비스를 활성화합니다. **Administration(관리)** > **System(시스템)** > **Deployment(구축)**를 선택한 후 노드를 열고 **General Settings(일반 설정)** 아래에서 **Enable Passive Identity Service(패시브 ID 서비스 활성화)** 및 **pxGrid**를 활성화합니다.
- ISE에 DNS(도메인 이름 서버)의 항목이 있는지 확인합니다. ISE에서 클라이언트 머신에 대 한 역방향 조회를 올바르게 구성했는지 확인합니다. 자세한 내용은 다음을 참조하십시오. DNS 서버, 46 페이지

단계 **1** **Work Centers(작업 센터)** > **PassiveID(패시브 ID)**를 선택합니다. Passive Identity Connector Overview(패시브 ID 커넥터 개요) 화면에서 **Passive Identity Wizard(패시브 ID 마법사)**를 클릭합니다.

그림 *11: PassiveID Setup(*패시브 *ID* 설정*)*



단계 **2** **Next(**다음**)**를 클릭하여 마법사를 시작합니다.

단계 **3** 이 Active Directory 조인 포인트의 고유한 이름을 입력합니다. 이 노드가 연결된 Active Directory 도메인의 도메인 이름을 입력하고 Active Directory 관리자의 사용자 이름과 비밀번호를 입력합니다. .

Store credentials(자격 증명 저장**)**는 되도록 선택하는 것이 좋습니다. 관리자의 사용자 이름이나 비밀번호가 저장되어 모니터링 용도로 구성되는 모든 DC(도메인 컨트롤러)에서 사용할 수 있습니다.

단계 **4** **Next(**다음**)**를 클릭하여 Active Directory 그룹을 정의하고 포함 및 모니터링할 사용자 그룹을 확인합니다.
Active Directory 사용자 그룹은 이전 단계에서 구성한 Active Directory 조인 포인트에 따라 자동으로 표시됩니다.

단계 **5** **Next(**다음**)**를 클릭합니다. 모니터링할 DC를 선택합니다. Custom(사용자 맞춤화)을 선택했다면 다음 화면에서 모니터링할 특정 DC를 선택합니다. 모두 마쳤으면 **Next(**다음**)**를 클릭합니다.

단계 **6** **Exit(**종료**)**를 클릭하여 마법사를 완료합니다.

다음에 수행할 작업

Active Directory를 초기 제공자로 구성하는 작업이 끝나면, 추가 제공자 유형도 쉽게 구성할 수 있습니다. 자세한 내용은 추가 패시브 ID 서비스 제공자, 94 페이지를 참고하십시오. 나아가 정의한 제공자가 수집하는 사용자 ID 정보를 수신하도록 지정된 가입자를 구성할 수도 있습니다. 자세한 내용은 가입자, 134 페이지를 참고하십시오.

Active Directory 제공자 관리

Active Directory 조인 포인트를 생성하고 구성했다면, 이러한 작업을 이용해 Active Directory 프로브를 관리해야 합니다.

- Active Directory Authentication(인증)용 Test Users(사용자 테스트), 61 페이지
- 노드의 Active Directory 가입 보기, 62 페이지
- Active Directory 문제 진단, 63 페이지
- Active Directory 도메인 탈퇴, 52 페이지
- Active Directory 컨피그레이션 삭제, 62 페이지
- Active Directory 디버그 로그 활성화, 64 페이지

Active Directory 설정

Active Directory(AD)는 사용자 이름과 IP 주소 같은 사용자 정보를 수신할 수 있는 대단히 안전하고 정확한 소스입니다.

조인 포인트를 생성하고 수정하여 Active Directory 프로브를 생성하고 관리하려면 **Work Centers(**작업 센터**)** > **PassiveID(**패시브 **ID)** > **Providers(**제공자**)** > **Active Directory**를 선택합니다.

자세한 내용은 Active Directory 가입 포인트를 추가하고 해당 가입 포인트에 Cisco ISE 노드 가입, 47 페이지를 참고하십시오.

표 ***16: Active Directory*** 조인 포인트 이름 설정 및 도메인 조인 창

필드 이름	설명
조인 포인트 이름	구성한 조인 포인트를 빠르고 쉽게 구분할 수 있는 고유한 이름입니다.
Active Directory 도메인	이 노드가 연결된 Active Directory 도메인의 도메인 이름입니다.

필드 이름	설명
도메인 관리자	관리자 권한이 있는 Active Directory 사용자의 사용자 원이름 또는 사용자 계정 이름입니다.
Password(비밀번호**)**	Active Directory에 구성한 도메인 관리자의 비밀번호입니다.
조직 단위 지정	관리자의 조직 단위 정보를 입력합니다.
자격 증명 저장	**Store credentials(**자격 증명 저장**)**는 되도록 선택하는 것이 좋습니다. 관리자의 사용자 이름이나 비밀번호가 저장되어 모니터링 용도로 구성되는 모든 DC(도메인 컨트롤러)에서 사용할 수 있습니다. 엔드포인트 프로브의 경우에는 **Store credentials(**자격 증명 저장**)**를 반드시 선택해야 합니다.

표 ***17: Active Directory*** 조인/탈퇴 창

필드 이름	설명
ISE Node(ISE 노드**)**	설치 내 특정 노드의 URL입니다.
ISE 노드 역할	노드가 설치 내 기본 노드인지 보조 노드인지를 나타냅니다.
Status(상태**)**	노드가 Active Directory 도메인에 적극적으로 가입했는지를 나타냅니다.
도메인 컨트롤러	Active Directory에 가입한 노드의 경우 이 열은 Active Directory 도메인에서 노드가 연결된 특정 도메인 컨트롤러를 나타냅니다.
사이트	Active Directory 포리스트가 ISE에 조인한 경우, 이 필드는 Active Directory Site & Services(Active Directory 사이트 및 서비스) 영역에 표시되는 포리스트 내의 특정 Active Directory 사이트를 나타냅니다.

표 ***18:*** 패시브 ***ID DC(***도메인 컨트롤러***)*** 목록

필드	설명
도메인	도메인 컨트롤러가 있는 서버의 정규화된 도메인 이름입니다.

필드	설명
DC 호스트	도메인 컨트롤러가 있는 호스트입니다.
사이트	Active Directory 포리스트가 ISE에 조인한 경우, 이 필드는 Active Directory Site & Services(Active Directory 사이트 및 서비스) 영역에 표시되는 포리스트 내의 특정 Active Directory 사이트를 나타냅니다.
IP Address(IP 주소**)**	도메인 컨트롤러의 IP 주소.
모니터링	다음 방법 중 하나를 사용하여 Active Directory 도메인 컨트롤러에서 사용자 ID 정보를 모니터링합니다. • WMI: WMI 인프라를 사용하여 Active Directory를 직접 모니터링합니다. • 에이전트 이름: Active Directory에서 사용자 정보를 모니터링하도록 에이전트를 정의한 경우, 에이전트 프로토콜을 선택하고 드롭다운 목록에서 사용할 에이전트를 선택합니다. 에이전트에 관한 자세한 내용은 Active Directory 에이전트, 97 페이지 항목을 참조하십시오.

표 ***19:*** 패시브 ***ID DC(Domain Controller,*** 도메인 컨트롤러***)*** 편집 화면

필드 이름	설명
호스트 **FQDN**	도메인 컨트롤러가 있는 서버의 정규화된 도메인 이름을 입력합니다.
Description(설명**)**	쉽게 식별할 수 있도록 이 도메인 컨트롤러에 관한 고유한 설명을 입력합니다.
사용자 이름	Active Directory에 액세스하는 데 사용하는 관리자의 사용자 이름입니다.
Password(비밀번호**)**	Active Directory에 액세스하는 데 사용하는 관리자의 비밀번호입니다.

필드 이름	설명
Protocol(프로토콜)	다음 방법 중 하나를 사용하여 Active Directory 도메인 컨트롤러에서 사용자 ID 정보를 모니터링합니다. • WMI: WMI 인프라를 사용하여 Active Directory를 직접 모니터링합니다. • 에이전트 이름: Active Directory에서 사용자 정보를 모니터링하도록 에이전트를 정의한 경우, 에이전트 프로토콜을 선택하고 드롭다운 목록에서 사용할 에이전트를 선택합니다. 에이전트에 관한 자세한 내용은 Active Directory 에이전트, 97 페이지 항목을 참조하십시오.

Active Directory 그룹은 Active Directory에서 정의하고 관리하며, 이 탭에서는 이 노드에 가입한 Active Directory의 그룹을 확인할 수 있습니다. Active Directory에 관한 자세한 내용은 https://msdn.microsoft.com/en-us/library/bb742437.aspx 항목을 참조하십시오.

표 ***20: Active Directory*** 고급 설정

필드 이름	설명
기록 간격	이미 수행된 사용자 로그인 정보를 패시브 ID 서비스에서 읽는 시간입니다. 패시브 ID 서비스를 시작하거나 재시작할 때 서비스를 사용할 수 없었던 시간 동안 생성된 이벤트를 확인하려면 이 시간을 설정해야 합니다. 활성 상태인 엔드포인트 프로브는 이 간격의 빈도를 유지합니다.
사용자 세션 에이징 타임	사용자가 로그인할 수 있는 시간입니다. 패시브 ID 서비스는 DC에서 새 사용자 로그인 이벤트를 식별하지만, DC는 사용자가 로그오프할 때는 보고하지 않습니다. 에이징 시간을 설정하면 Cisco ISE는 사용자가 로그인되어 있는 시간 간격을 확인할 수 있습니다.
NTLM 프로토콜 설정	Cisco ISE와 DC 간의 통신 프로토콜로는 NTLMv1 또는 NTLMv2를 선택할 수 있습니다. NTLMv2rk 권장 기본값입니다.

추가 패시브 ID 서비스 제공자

ISE가 서비스에 가입한 고객(가입자)에게 ID 정보를 제공하게 하려면(패시브 ID 서비스) , 먼저 ID 제공자에 연결되는 ISE 프로브를 구성해야 합니다.

매핑되고 ISE에 정보를 적극적으로 전달하는 제공자는 Live Sessions(라이브 세션) 메뉴의 세션 디렉토리에서 확인할 수 있습니다. Live Sessions(라이브 세션)에 관한 자세한 내용은 RADIUS 라이브 세션 항목을 참조하십시오.

아래 표에는 ISE에서 사용 가능한 모든 제공자 및 프로브 유형에 대한 세부정보가 나와 있습니다. Active Directory에 관한 자세한 내용은 프로브 및 제공자로서의 Active Directory, 88 페이지 항목을 참조하십시오.

다음과 같은 제공자 유형을 정의할 수 있습니다.

표 *21:* 제공자 유형

제공자 유형(프로브)	설명	소스 시스템(제공자)	기술	수집한 사용자 ID 정보	문서 링크
AD(Active Directory)	대단히 안전하고 정확하며 가장 자주 사용하는 소스로, 사용자 정보를 수신하는 곳입니다. 프로브로서 AD는 WMI 기술을 이용해, 인증된 사용자 ID를 전달합니다. 프로브로서가 아닌 AD 자체는 다른 프로브가 사용자 데이터를 검색하는 소스 시스템(제공자) 역할을 합니다.	Active Directory 도메인 컨트롤러	WMI	• 사용자 이름 • IP 주소 • 도메인	프로브 및 제공자로서의 Active Directory, 88 페이지
에이전트	Active Directory 도메인 컨트롤러 또는 멤버 서버에 설치된 네이티브 32비트 애플리케이션입니다. 에이전트 프로브는 Active Directory를 사용하여 사용자 ID 정보를 확인하는 신속하고 효율적인 솔루션입니다.		도메인 컨트롤러 또는 멤버 서버에 설치된 에이전트입니다.	• 사용자 이름 • IP 주소 • 도메인	Active Directory 에이전트, 97 페이지
엔드포인트	다른 구성된 프로브와 함께 백그라운드에서 항상 실행되어 사용자가 여전히 연결되어 있는지를 확인합니다.		WMI	사용자가 계속 연결되어 있는지 여부	엔드포인트 프로브, 131 페이지
SPAN			SPAN(스위치에 설치됨) 및 Kerberos 메시지	• 사용자 이름 • IP 주소 • 도메인	SPAN, 107 페이지

제공자 유형(프로브)	설명	소스 시스템(제공자)	기술	수집한 사용자 ID 정보	문서 링크
	네트워크 트래픽을 수신 대기하기 위해 네트워크 스위치에 상주하며, Active Directory 데이터를 기반으로 사용자 ID 정보를 추출합니다.				
API 제공자	ISE가 제공하는 RESTful API 서비스를 이용하여, RESTful API 클라이언트와 통신하도록 프로그래밍된 모든 시스템에서 사용자 ID 정보를 수집합니다.	REST API 클라이언트와 통신하도록 프로그래밍된 모든 시스템입니다.	RESTful API. 가입자에게 전송된 JSON 형식의 사용자 ID.	• 사용자 이름 • IP 주소 • 포트 범위 • 도메인	API Providers(API 제공자), 102 페이지
Syslog	시스템 로그 메시지를 구문 분석하고 MAC 주소를 포함한 사용자 ID를 검색합니다.	• 일반 시스템 로그 메시지 제공자 • DHCP 서버	시스템 로그 메시지	• 사용자 이름 • IP 주소 • MAC 주소 • 도메인	Syslog Providers(시스템 로그 제공자), 109 페이지

Active Directory 에이전트

패시브 ID 서비스 작업 센터는 네이티브 32비트 애플리케이션인 Domain Controller(DC) 에이전트를 Active Directory(AD) 도메인 컨트롤러(DC) 또는 (컨피그레이션에 따라) 멤버 서버에 설치하여 AD에서 사용자 ID 정보를 검색한 다음, 이러한 ID를 사용자가 구성한 가입자에게 전송합니다. 에이전트 프로브는 Active Directory를 사용하여 사용자 ID 정보를 확인하는 신속하고 효율적인 솔루션입니다. 에이전트는 별도의 도메인 또는 AD 도메인에 설치할 수 있으며, 설치한 후에는 1분마다 한 번씩 ISE에 상태 업데이트를 제공합니다.

에이전트는 ISE가 자동으로 설치 및 구성하며, 사용자가 수동으로 설치할 수도 있습니다. 설치하면 다음과 같은 일이 발생합니다.

- 에이전트와 관련 파일이 **`Program Files/Cisco/Cisco ISE PassiveID Agent`** 경로에 설치됩니다.

- 에이전트의 로깅 수준을 보여주는 **PICAgent.exe.config**라는 구성 파일이 설치됩니다. 구성 파일에서 로깅 레벨을 수동으로 변경할 수 있습니다.
- CiscoISEPICAgent.log 파일은 모든 로깅 메시지와 함께 저장됩니다.
- nodes.txt 파일에는 에이전트가 통실할 수 있는 구축 내 모든 노드 목록이 있습니다. 에이전트가 목록의 첫 번째 노드에 접촉합니다. 노드에 접촉할 수 없는 경우 에이전트는 목록의 노드 순서에 따라 계속 통신을 시도합니다. 수동 설치의 경우에는 파일을 열고 노드 IP 주소를 입력해야 합니다. (수동 또는 자동으로) 설치가 끝난 후에는 파일을 변경하려면 수동으로 업데이트해야 합니다. 필요하다면 파일을 열고 노드 IP 주소를 추가, 변경 또는 삭제합니다.
- Cisco ISE PassiveID 에이전트 서비스는 Windows Services 대화 상자에서 관리할 수 있는 머신에서 실행됩니다.
- ISE는 도메인 컨트롤러를 100개까지 지원하며, 각 에이전트는 도메인 컨트롤러를 10개까지 모니터링할 수 있습니다.

참고 도메인 컨트롤러 100개를 모니터링하려면 에이전트 10개를 구성해야 합니다.

참고 Active Directory 에이전트는 Windows Server 2008 이상에서만 지원됩니다.

에이전트를 설치할 수 없는 경우에는 패시브 ID 서비스에 Active Directory 프로브를 사용합니다. 자세한 내용은 프로브 및 제공자로서의 Active Directory, 88 페이지를 참고하십시오.

Active Directory 에이전트 자동 설치 및 구축

도메인 컨트롤러에서 사용자 ID를 모니터링하도록 에이전트 제공자를 구성하는 경우 에이전트를 멤버 서버 또는 도메인 컨트롤러에 설치해야 합니다. 에이전트는 ISE에서 자동으로 설치하거나 사용자가 수동으로 설치할 수 있습니다. 자동 또는 수동 설치 후에는 기본 WMI가 아닌 지정된 도메인 컨트롤러를 모니터링하도록 설치된 에이전트를 구성해야 합니다. 이 프로세스에서는 자동 설치를 활성화하고 도메인 컨트롤러를 모니터링하도록 에이전트를 구성하는 방법을 설명합니다.

시작하기 전에

시작하기 전에

- 서버 측에서 관련 DNS 서버에 대한 역방향 조회를 구성합니다. ISE의 DNS 서버 구성 요구 사항에 관한 자세한 내용은 DNS 서버, 46 페이지 항목을 참조하십시오.
- 에이전트에 지정된 머신에서 Microsoft.NET Framework가 4.0 이상 버전으로 업데이트되었는지 확인합니다. .NET Framework에 대한 자세한 내용은 https://www.microsoft.com/net/framework 항목을 참고하십시오.

- 패시브 ID 및 pxGrid 서비스를 활성화합니다. 자세한 내용은 초기 설정 및 컨피그레이션, 86 페이지를 참고하십시오.
- AD 조인 포인트를 생성하고 하나 이상의 도메인 컨트롤러를 추가합니다. 조인 포인트에 관한 자세한 내용은 프로브 및 제공자로서의 Active Directory, 88 페이지 항목을 참고하십시오.

  AD 사용자 그룹을 AD, 에이전트, SPAN 및 시스템 로그 프로브에 사용합니다. AD 그룹에 관한 자세한 내용은 Active Directory 사용자 그룹 구성, 54 페이지 항목을 참조하십시오.

단계 **1** **Work Centers(**작업 센터**)** > **PassiveID(**패시브 **ID)** > **Providers(**제공자**)**를 선택하고 왼쪽 패널에서 **Agents(**에이전트**)**를 선택합니다.

단계 **2** 새 에이전트를 추가하려면 표 상단에 있는 **Add(**추가**)**를 클릭합니다.

단계 **3** 새 에이전트를 생성하고 이 구성에서 지정한 호스트에 자동으로 설치하려면 **Deploy New Agent(**새 에이전트 구축**)**를 선택합니다.

단계 **4** 모든 필수 필드를 올바르게 작성하여 클라이언트를 올바르게 구성합니다. 자세한 내용은 Active Directory 에이전트 설정, 101 페이지를 참고하십시오.

단계 **5** **Deploy(**구축**)**를 클릭합니다.
에이전트는 구성에서 지정한 도메인에 따라 호스트에 자동으로 설치되며 설정이 저장됩니다. 이제 에이전트가 Agents(에이전트) 표에도 표시되며 다음 단계에 설명된 대로 지정된 도메인 컨트롤러를 모니터링하는 데 적용 가능합니다.

단계 **6** **Work Centers(**작업 센터**)** > **PassiveID(**패시브 **ID)** > **Providers(**제공자**)**를 선택하고 왼쪽 패널에서 **Active Directory**를 선택하여 현재 구성된 모든 조인 포인트를 확인합니다.

단계 **7** 생성한 에이전트를 활성화할 조인 포인트의 링크를 클릭합니다.

단계 **8** **Passive ID(**패시브 **ID)** 탭을 선택하여 사전 요건에 따라 추가한 도메인 컨트롤러를 구성합니다.

단계 **9** 생성한 에이전트로 모니터링할 도메인 컨트롤러를 선택하고 **Edit(**편집**)**를 클릭합니다.

단계 **10** **Protocol(**프로토콜**)** 드롭다운 목록에서 **Agent(**에이전트**)**를 선택합니다.

단계 **11** **Agent(**에이전트**)** 드롭다운 목록에서 생성한 에이전트를 선택합니다. 에이전트에 대해 생성한 사용자 이름 및 비밀번호 자격 증명(있는 경우)을 입력하고 **Save(**저장**)**를 클릭합니다.

Active Directory 에이전트 수동 설치 및 구축

도메인 컨트롤러에서 사용자 ID를 모니터링하도록 에이전트 제공자를 구성하는 경우 에이전트를 멤버 서버 또는 도메인 컨트롤러에 설치해야 합니다. 에이전트는 ISE에서 자동으로 설치하거나 사용자가 수동으로 설치할 수 있습니다. 자동 또는 수동 설치 후에는 기본 WMI가 아닌 지정된 도메인 컨트롤러를 모니터링하도록 설치된 에이전트를 구성해야 합니다. 이 프로세스에서는 도메인 컨트롤러를 모니터링하도록 에이전트를 수동으로 설치하고 구성하는 방법을 설명합니다.

시작하기 전에

시작하기 전에

- 서버 측에서 관련 DNS 서버에 대한 역방향 조회를 구성합니다. ISE의 DNS 서버 구성 요구 사항에 관한 자세한 내용은 DNS 서버, 46 페이지 항목을 참조하십시오.

- 에이전트에 지정된 머신에서 Microsoft.NET Framework가 4.0 이상 버전으로 업데이트되었는지 확인합니다. .NET Framework에 대한 자세한 내용은 https://www.microsoft.com/net/framework 항목을 참고하십시오.
- 패시브 ID 및 pxGrid 서비스를 활성화합니다. 자세한 내용은 초기 설정 및 컨피그레이션, 86 페이지를 참고하십시오.
- AD 조인 포인트를 생성하고 하나 이상의 도메인 컨트롤러를 추가합니다. 조인 포인트에 관한 자세한 내용은 프로브 및 제공자로서의 Active Directory, 88 페이지 항목을 참고하십시오.

  AD 사용자 그룹을 AD, 에이전트, SPAN 및 시스템 로그 프로브에 사용합니다. AD 그룹에 관한 자세한 내용은 Active Directory 사용자 그룹 구성, 54 페이지 항목을 참조하십시오.

단계 **1** **Work Centers**(작업 센터) > **PassiveID**(패시브 **ID**) > **Providers**(제공자)를 선택하고 왼쪽 패널에서 **Agents**(에이전트)를 선택합니다.

단계 **2** **Download Agent**(에이전트 다운로드)를 클릭하여 수동 설치를 위한 **`pxagent-installer.zip`** 파일을 다운로드합니다.
파일은 기본 Windows 다운로드 폴더에 다운로드됩니다.

단계 **3** 지정된 호스트 머신에 zip 파일을 배치하고 설치를 실행합니다.

단계 **4** ISE GUI에서 다시 **Work Centers**(작업 센터) > **PassiveID**(패시브 **ID**) > **Providers**(제공자)를 선택하고 왼쪽 패널에서 **Agents**(에이전트)를 선택합니다.

단계 **5** 새 에이전트를 구성하려면 표 상단에 있는 **Add**(추가)를 클릭합니다.

단계 **6** 호스트 머신에 이미 설치한 에이전트를 구성하려면 **Register Existing Agent**(기존 에이전트 등록)를 선택합니다.

단계 **7** 모든 필수 필드를 올바르게 작성하여 클라이언트를 올바르게 구성합니다. 자세한 내용은 Active Directory 에이전트 설정, 101 페이지를 참고하십시오.

단계 **8** **Save**(저장)를 클릭합니다.
에이전트 설정이 저장됩니다. 이제 에이전트가 Agents(에이전트) 표에도 표시되며 다음 단계에 설명된 대로 지정된 도메인 컨트롤러를 모니터링하는 데 적용 가능합니다.

단계 **9** **Work Centers**(작업 센터) > **PassiveID**(패시브 **ID**) > **Providers**(제공자)를 선택하고 왼쪽 패널에서 **Active Directory**를 선택하여 현재 구성된 모든 조인 포인트를 확인합니다.

단계 **10** 생성한 에이전트를 활성화할 조인 포인트의 링크를 클릭합니다.

단계 **11** **Passive ID**(패시브 **ID**) 탭을 선택하여 사전 요건에 따라 추가한 도메인 컨트롤러를 구성합니다.

단계 **12** 생성한 에이전트로 모니터링할 도메인 컨트롤러를 선택하고 **Edit**(편집)를 클릭합니다.

단계 **13** **Protocol**(프로토콜) 드롭다운 목록에서 **Agent**(에이전트)를 선택합니다.

단계 **14** **Agent**(에이전트) 드롭다운 목록에서 생성한 에이전트를 선택합니다. 에이전트에 대해 생성한 사용자 이름 및 비밀번호 자격 증명(있는 경우)을 입력하고 **Save**(저장)를 클릭합니다.

에이전트 제거

자동 또는 수동으로 설치된 에이전트는 Windows에서 직접 쉽게(수동으로) 제거할 수 있습니다.

단계 **1** Windows 대화 상자에서 **Programs and Features(**프로그램 및 기능**)**로 이동합니다.
단계 **2** 설치된 프로그램 목록에서 Cisco ISE PassiveID 에이전트를 찾아 선택합니다.
단계 **3** **Uninstall(**제거**)**을 클릭합니다.

Active Directory 에이전트 설정

서로 다른 DC(Domain Controller)에서 사용자 ID 정보를 검색하고 패시브 ID 서비스 가입자에게 해당 정보를 전달하려면 ISE가 네트워크의 지정된 호스트에 에이전트를 자동으로 설치하도록 허용합니다.

에이전트를 생성 및 관리하려면 **Providers(**제공자**)** > **Agents(**에이전트**)**를 선택합니다. Active Directory 에이전트 자동 설치 및 구축, 98 페이지의 내용을 참조하십시오.

표 ***22: Agents(***에이전트***)*** 창

필드 이름	설명
Name(이름**)**	구성한 에이전트 이름입니다.
Host(호스트**)**	에이전트가 설치된 호스트의 FQDN(Fully Qualified Domain Name)입니다.
Monitoring(모니터링**)**	지정된 에이전트가 모니터링 중인 도메인 컨트롤러의 쉼표로 구분된 목록입니다.

표 ***23:*** 에이전트 신규

필드	설명
새 에이전트 구축 또는 기존 에이전트 등록	• Deploy New Agent(새 에이전트 구축): 지정된 호스트에 새 에이전트를 설치합니다. • Register Existing Agent(기존 에이전트 등록): 호스트에 에이전트를 수동으로 설치한 다음 패시브 ID 서비스의 이 화면에서 해당 에이전트를 구성하여 서비스를 활성화합니다.
Name(이름**)**	에이전트를 쉽게 인식할 수 있는 이름을 입력합니다.
Description(설명**)**	에이전트를 쉽게 인식할 수 있는 설명을 입력합니다.
Host FQDN(호스트 **FQDN)**	이는 에이전트가 설치된(기존 에이전트 등록) 호스트가 설치될(자동 구축) 호스트의 FQDN(Fully Qualified Domain Name)입니다.

필드	설명
User Name(사용자 이름**)**	에이전트를 설치할 호스트에 액세스하려면 사용자 이름을 입력합니다. 패시브 ID 서비스는 이러한 인증서를 사용하여 에이전트를 설치합니다.
Password(비밀번호**)**	에이전트를 설치할 호스트에 액세스하려면 비밀번호를 입력합니다. 패시브 ID 서비스는 이러한 인증서를 사용하여 에이전트를 설치합니다.

API Providers(API 제공자)

Cisco ISE에서 API Providers(API 제공자) 기능을 이용하면 맞춤형 프로그램이나 터미널 서버(TS)-Agent에서 얻은 사용자 ID 정보를 내장된 ISE passive identity services(ISE 패시브 ID 서비스) REST API 서비스로 푸시할 수 있습니다. 이렇게 하면 네트워크에서 프로그램 가능 클라이언트를 맞춤화하여 아무 NAC(Network Access Control) 시스템에서 수집한 사용자 ID를 서비스로 전송할 수 있습니다. 또한 Cisco ISE API 제공자를 이용하면 모든 사용자가 IP 주소는 같지만 고유한 포트에 할당되는 Citrix 서버에서 TS-Agent 같은 네트워크 애플리케이션에 접속할 수 있습니다.

예를 들어 Active Directory(AD) 서버를 대상으로 인증된 사용자의 ID 매핑을 제공하는 Citrix 서버에서 실행하는 에이전트는 REST 요청을 ISE에 전송하여, 새 사용자가 로그인 또는 로그오프할 때마다 사용자 세션을 추가 또는 삭제할 수 있습니다. 그러면 ISE는 클라이언트에서 전달한, IP 주소와 할당된 포트를 포함한 사용자 ID 정보를 얻은 다음 Cisco FMC(Firepower Management Center) 같은 사전 구성한 가입자에 전송합니다.

ISE REST API 프레임워크는 HTTPS 프로토콜로 REST 서비스를 구현하며(클라이언트 인증서 검증 필요 없음), 사용자 ID 정보는 JSON(JavaScript Object Notation) 형식으로 제공됩니다. JSON에 관한 자세한 내용은 http://www.json.org/ 항목을 참조하십시오.

ISE REST API 서비스는 사용자 ID를 구문 분석하고, 이 정보를 포트 범위에 매핑하여 같은 시스템에 동시에 로그인한 사용자를 구분합니다. 포트가 사용자에게 할당될 때마다 API는 ISE에 메시지를 보냅니다.

REST API 제공자 흐름

클라이언트를 ISE의 제공자로 선언하고 해당하는 맞춤형 프로그램(클라이언트)이 RESTful 요청을 전송할 수 있도록 ISE에서 맞춤형 클라이언트로 이어지는 브리지를 구성하면, ISE REST 서비스는 다음 방식으로 작동하게 됩니다.

1. 클라이언트 인증의 경우 Cisco ISE는 인증 토큰을 요구합니다. 클라이언트 머신의 맞춤형 프로그램은 연락처를 초기화할 때 인증 토큰 요청을 전송하며, 이후에는 이전 토큰이 만료될 때마다 ISE가 이를 알립니다. 요청의 응답으로 토큰이 반환되어 클라이언트와 ISE 서비스 간에 진행 중인 통신을 활성화합니다.
2. 사용자가 네트워크에 로그인하면 클라이언트는 사용자 ID 정보를 검색하고 API Add 명령을 사용하여 ISE REST 서비스에 정보를 게시합니다.
3. Cisco ISE가 사용자 ID 정보를 수신하고 매핑합니다.

4. Cisco ISE가 매핑된 사용자 ID 정보를 가입자에게 전송합니다.
5. 맞춤형 머신은 필요할 때마다 Remove API 호출을 전송하고 전송한 Add 호출의 응답으로 수신한 사용자 ID를 포함하여, 사용자 정보 제거 요청을 전송할 수 있습니다.

ISE에서 **REST API Providers(REST API** 제공자**)**를 이용한 작업

ISE에서 REST 서비스를 활성화하려면 다음 단계를 따르십시오.

1. 클라이언트 측을 구성합니다. 자세한 내용은 클라이언트 사용 설명서를 참조하십시오.
2. 패시브 ID 및 pxGrid 서비스를 활성화합니다. 자세한 내용은 초기 설정 및 컨피그레이션, 86 페이지를 참고하십시오.
3. DNS 서버를 올바르게 구성했는지 확인합니다(ISE에서의 클라이언트 머신에 대한 역방향 조회 구성 포함). 의 DNS 서버 구성 요건에 관한 자세한 내용은 DNS 서버, 46 페이지 항목을 참조하십시오.
4. 패시브 ID 서비스용 ISE REST 서비스에 대한 Bridge(브리지)를 구성합니다., 103 페이지를 참조하십시오.

참고 TS-Agent와 함께 작동하도록 API Provider(API 제공자)를 설정하려면, ISE와 에이전트를 연결하는 브리지를 만들 때 TS-Agent를 추가한 다음 TS-Agent 설명서에서 API 호출 전송 관련 정보를 참조하십시오.

5. 인증 토큰을 생성하고 추가 및 제거 요청을 API 서비스에 전송합니다.

패시브 ID 서비스용 ISE REST 서비스에 대한 Bridge(브리지)를 구성합니다.

ISE REST API 서비스가 특정 클라이언트의 정보를 수신하게 하려면, 먼저 Cisco ISE에서 특정 클라이언를 정의해야 합니다. 서로 다른 IP 주소를 사용하여 여러 REST API 클라이언트를 정의할 수 있습니다.

시작하기 전에

시작하기 전에

- Passive ID(패시브 ID) 및 pxGrid 서비스를 활성화해야 합니다. 자세한 내용은 초기 설정 및 컨피그레이션, 86 페이지를 참고하십시오.
- DNS 서버를 올바르게 구성했는지 확인합니다(Cisco ISE에서의 클라이언트 머신에 대한 역방향 조회 구성 포함). Cisco ISE의 DNS 서버 구성 요구 사항에 관한 자세한 내용은 DNS 서버, 46 페이지 항목을 참고하십시오.

단계 **1** **Work Centers(**작업 센터**)** > **PassiveID(**패시브 **ID)** > **Providers(**제공자**)**를 선택하고 왼쪽 패널에서 **API Providers(API** 제공자**)**를 선택합니다.

각 기존 클라이언트에 관한 상태 정보를 포함하는 API Providers(API 제공자) 표가 표시됩니다.

단계 2 새 클라이언트를 추가하려면 표 상단에 있는 **Add(추가)**를 클릭합니다.

단계 3 모든 필수 필드를 올바르게 작성하여 클라이언트를 올바르게 구성합니다. 자세한 내용은 API 제공자 설정, 104 페이지를 참고하십시오.

단계 4 **Submit(제출)**을 클릭합니다.
클라이언트 구성이 저장되고 화면에 업데이트된 API Providers(API 제공자) 표가 표시됩니다. 이제 클라이언트가 ISE REST 서비스에 게시물을 보낼 수 있습니다.

다음에 수행할 작업

ISE REST 서비스에 인증 토큰과 사용자 ID를 게시하도록 사용자 맞춤화 클라이언를 설정합니다. 패시브 ID REST Service로 API Calls(API 호출) 전송, 104 페이지의 내용을 참조하십시오.

패시브 ID REST Service로 API Calls(API 호출) 전송

시작하기 전에

패시브 ID 서비스용 ISE REST 서비스에 대한 Bridge(브리지)를 구성합니다., 103 페이지

단계 1 브라우저의 주소 표시줄에서 Cisco ISE URL을 입력합니다(예: *https://<ise* 호스트 이름 또는 *IP* 주소*>/admin/*).

단계 2 **API Providers(API 제공자)** 창에서 지정하고 구성한 사용자 이름과 비밀번호를 입력합니다. 자세한 내용은 패시브 ID 서비스용 ISE REST 서비스에 대한 Bridge(브리지)를 구성합니다., 103 페이지를 참고하십시오.

단계 3 **Enter** 키를 누릅니다.

단계 4 대상 노드의 URL Address(URL 주소) 필드에 API 호출을 입력합니다.

단계 5 **Send(전송)**을 클릭하여 API 호출을 실행합니다.

다음에 수행할 작업

디양한 API 호출과 관련 스키마 및 결과에 관한 자세한 내용과 세부정보는 API 호출, 105 페이지 항목을 참조하십시오.

API 제공자 설정

참고 전체 API 정의 및 개체 스키마는 다음과 같이 요청 호출을 사용하여 검색할 수 있습니다.

- 전체 API 사양의 경우(wadl)—https://YOUR_ISE:9094/application.wadl
- API 모델 및 개체 스키마의 경우—https://YOUR_ISE:9094/application.wadl/xsd0.xsd

표 ***24: API*** 제공자 설정

필드	설명
Name(이름)	이 클라이언트를 다른 클라이언트와 쉽고 빠르게 구별할 수 있는 고유한 이름을 입력합니다.
설명	이 클라이언트에 관한 명확한 설명을 입력합니다.
상태	**Enabled(**활성**)**를 선택하면 구성 완료와 동시에 클라이언트가 REST 서비스와 상호작용합니다.
호스트/IP	클라이언트 호스트 머신의 IP 주소를 입력합니다. DNS 서버를 올바르게 구성했는지 확인합니다(ISE에서의 클라이언트 머신에 대한 역방향 조회 구성 포함).
사용자 이름	REST 서비스에 게시할 때 사용할 고유한 사용자 이름을 생성합니다.
Password(비밀번호)	REST 서비스에 게시할 때 사용할 고유한 비밀번호를 생성합니다.

API 호출

Cisco ISE로 패시브 ID 서비스용 사용자 ID 이벤트를 관리하려면 이러한 API 호출을 사용합니다.

목적: 인증 토큰 생성

- 요청

  POST

  https://<PIC IP address>:9094/api/fmi_platform/v1/identityauth/generatetoken

  요청에는 BasicAuth 권한 부여 헤더가 포함되어야 합니다. 이전에 ISE-PIC GUI에서 생성한 API 제공자의 자격 증명을 제공합니다. 자세한 내용은 API 제공자 설정, 104 페이지를 참조하십시오.

- 응답 헤더

  헤더에는 X-auth-access-token이 포함됩니다. 추가 REST 요청을 게시할 때 사용하는 토큰입니다.

- 응답 본문

  HTTP 204 No Content

목적: 사용자 추가

- 요청

  POST

  https://<PIC IP address>:9094/api/identity/v1/identity/useridentity

POST 요청 헤더에 X-auth-access-token을 추가합니다(예: 헤더: X-auth-access-token, 값: f3f25d81-3ac5-43ee-bbfb-20955643f6a7).

- 응답 헤더

  201 Created

- 응답 본문

  {

  "user": "<사용자 이름>",

  "srcPatRange": {

  "userPatStart": <사용자 PAT 시작 값>,

  "userPatEnd": <사용자 PAT 종료 값>,

  "patRangeStart": <PAT 범위 시작 값>

  },

  "srcIpAddress": "<src IP 주소>",

  "agentInfo": "<에이전트 이름>",

  "timestamp": "<ISO_8601 형식, 즉 “YYYY-MM-DDTHH:MM:SSZ" >",

  "domain": "<도메인>"

  }

- 메모
  - 위의 json에서 srcPatRange를 제거하면 단일 IP 사용자 바인딩을 생성할 수 있습니다.
  - 응답 본문에는 생성된 사용자 세션 바인딩에 대한 고유 식별자인 'ID'가 포함됩니다. DELETE 요청을 보낼 때 이 ID를 사용하여 제거 대상 사용자를 표시합니다.
  - 이 응답에는 새로 생성된 사용자 세션 바인딩의 URL인 자체 링크도 포함됩니다.

목적: 사용자 제거

- 요청

  DELETE

  https://<PIC IP address>:9094/api/identity/v1/identity/useridentity/<id>

  <id>에는 Add(추가) 응답에서 수신한 ID를 입력합니다.

  DELETE 요청 헤더에 X-auth-access-token 토큰을 추가합니다(예: 헤더: X-auth-access-token, 값: f3f25d81-3ac5-43ee-bbfb-20955643f6a7).

- 응답 헤더

  200 OK

- 응답 본문

응답 본문에는 삭제된 사용자 세션 바인딩 관련 세부정보가 포함됩니다.

SPAN

SPAN은 패시브 ID 서비스Cisco ISE에서 직접 작동하도록 Active Directory를 구성하지 않고도 네트워크를 수신 대기하고 사용자 정보를 검색하도록 Cisco ISE를 빠르고 쉽게 활성화할 수 있는 입니다. SPAN은 네트워크 트래픽을, 특히 Kerberos 메시지를 검사하고 Active Directory에 저장된 사용자 ID 정보를 추출한 다음 정보를 ISE로 전송합니다. 그러면 ISE는 정보를 구문 분석하고, ISE에서 이전에 구성한 가입자에게 사용자 이름, IP 주소와 도메인 이름을 최종 전달합니다.

SPAN이 네트워크를 수신 대기하고 Active Directory 사용자 정보를 추출하려면, ISE와 Active Directory 모두가 네트워크에서 같은 스위치에 연결되어야 합니다. 이렇게 하면 SPAN은 Active Directory에서 모든 사용자 ID 데이터를 복사하고 미러링할 수 있습니다.

SPAN을 사용하면 사용자 정보를 다음 방법으로 검색합니다.

1. 사용자 엔드포인트에서 네트워크에 로그인합니다.
2. 로그인 및 사용자 데이터가 Kerberos 메시지에 저장됩니다.
3. 사용자가 로그인하고 사용자 데이터가 스위치를 통과하면, SPAN이 네트워크 데이터를 미러링합니다.
4. Cisco ISE가 네트워크에서 사용자 정보를 수신 대기하고 스위치에서 미러링된 데이터를 검색합니다.
5. Cisco ISE가 사용자 정보를 구문 분석하고 패시브 ID 매핑을 업데이트합니다.
6. Cisco ISE가 구문 분석된 사용자 정보를 가입자에게 전달합니다.

SPAN으로 작업

시작하기 전에

ISE가 네트워크 스위치에서 SPAN 트래픽을 수신하도록 설정하려면 먼저 스위치를 수신 대기할 노드와 노드 인터페이스를 정의해야 합니다. 설치된 서로 다른 ISE 노드를 SPAN이 수신 대기하도록 구성할 수 있습니다. 각 노드에 대해 하나의 인터페이스만 네트워크를 수신하도록 구성할 수 있으며, 수신하는 데 사용되는 인터페이스는 SPAN 전용이어야 합니다.

시작하기 전에 Passive ID(패시브 ID) 및 pxGrid 서비스를 활성화해야 합니다. SPAN 구성에 사용 가능한 인터페이스 목록에는 패시브 ID가 활성화된 노드만 나타납니다. 자세한 내용은 초기 설정 및 컨피그레이션, 86 페이지를 참고하십시오.

또한 다음을 수행해야 합니다.

- 네트워크에 Active Directory가 구성되어 있는지 확인합니다.
- 스위치가 ISE와 통신할 수 있도록, Active Directory에도 연결된 네트워크의 스위치에서 CLI를 실행합니다.
- AD에서 네트워크를 미러링하도록 스위치를 구성합니다.

- SPAN용 전용 ISE NIC(네트워크 인터페이스 카드)를 구성합니다. 이 NIC는 SPAN 트래픽에만 사용됩니다.
- SPAN 전용 NIC가 명령줄 인터페이스를 통해 활성화되었는지 확인합니다.
- Kerberos 트래픽만 SPAN 포트로 전송하는 VACL을 생성합니다.

단계 **1** **Work Centers(**작업 센터**)** > **PassiveID(**패시브 **ID)** > **Providers(**제공자**)**를 선택하고 왼쪽 창에서 **SPAN**을 선택해 SPAN을 구성합니다.

단계 **2** 참고 GigabitEthernet0 NIC(네트워크 인터페이스 카드)는 계속 사용 가능한 상태로 유지하고 SPAN 구성 시에는 사용 가능한 다른 NIC를 선택하는 것이 좋습니다. GigabitEthernet0은 시스템 관리 목적으로 사용됩니다.

의미 있는 설명(선택 사항)을 입력하고 **Enabled(**활성화됨**)** 상태를 선택한 다음 네트워크 스위치를 수신하는 데 사용할 노드 및 관련 NIC를 선택합니다. 자세한 내용은 SPAN 설정, 108 페이지를 참고하십시오.

단계 **3** **Save(**저장**)**를 클릭합니다.
SPAN 컨피그레이션이 저장되고 ISE가 현재 네트워크 트래픽을 수신 대기하고 있습니다.ISE-PIC

SPAN 설정

구축한 각 노드에서 클라이언트 네트워크에 SPAN을 설치하여, ISE가 사용자 ID를 수신하도록 빠르고 쉽게 구성합니다.

표 ***25: SPAN*** 설정

필드	설명
Description(설명**)**	현재 활성화된 노드 및 인터페이스를 구별할 수 있는 고유한 설명을 입력합니다.
Status(상태**)**	**Enabled(**활성**)**를 선택하면 구성 완료와 동시에 클라이언트를 활성화합니다.
인터페이스 **NIC**	ISE에 설치된 노드를 하나 이상 선택한 다음, 선택한 각 노드에 대해 네트워크 정보를 수신할 노드 인터페이스를 선택합니다. 참고 GigabitEthernet0 NIC는 사용 가능한 상태로 유지하고 SPAN 구성에는 사용 가능한 다른 NIC를 선택하는 것이 좋습니다. GigabitEthernet0은 시스템 관리 목적으로 사용됩니다.

Syslog Providers(시스템 로그 제공자)

패시브 ID 서비스 (InfoBlox, Blue Coat, BlueCat, Lucent 등의 제공자가 보낸) 일반 시스템 로그와 DHCP 시스템 로그 메시지를 포함한 시스템 메시지를 전달하는 클라이언트(ID 데이터 제공자)가 보낸 시스템 로그 메시지를 구문 분석하고, MAC 주소를 포함한 사용자 ID 정보를 다시 전송합니다. 그러면 매핑된 사용자 ID 데이터가 가입자에게 전달됩니다.

사용자 ID 데이터를 수신할 시스템 로그 클라이언트를 지정할 수 있습니다(시스템 로그 클라이언트 구성, 109 페이지 참고). 제공자를 구성할 때 관리자는 연결 방법(TCP 또는 UDP)과 구문 분석에 사용할 시스템 로그 템플릿을 지정해야 합니다.

참고

TCP가 구성된 연결 유형이며 메시지 헤더에 문제가 있어 호스트 이름을 구문 분석할 수 없다면, ISE는 패킷에서 수신한 IP 주소를 ISE의 시스템 로그 메시지에 구성된 제공자 목록에 있는 IP 주소와 일치시킵니다. 이 목록을 보려면 **Work Centers(**작업 센터**)** > **PassiveID(**패시브 **ID)** > **Providers(**제공자**)** > **Syslog Providers(**시스템 로그 제공자**)**를 선택합니다. 구문 분석 성공을 보장하려면 메시지 헤더를 확인하고 필요하다면 사용자 맞춤화하는 것이 좋습니다. 헤더 사용자 맞춤화에 관한 자세한 내용은 시스템 로그 헤더 사용자 맞춤화, 116 페이지 항목을 참조하십시오.

시스템 로그 프로브는 수신한 메시지를 ISE 구문 분석기로 전송하고, 구문 분석기는 사용자 ID 정보를 매핑한 다음 정보를 ISE에 게시합니다. 그런 다음 ISE가 구분 분석과 매핑이 끝난 사용자 ID 정보를 패시브 ID 서비스 가입자에게 전달합니다.

ISE-PIC ISE에서 사용자 ID의 시스템 로그 메시지를 구문 분석하려면 다음을 수행하십시오.

- 사용자 ID 데이터를 받을 시스템 로그 클라이언트를 구성합니다. 시스템 로그 클라이언트 구성, 109 페이지의 내용을 참조하십시오.
- 단일 메시지 헤더를 사용자 맞춤화합니다. 시스템 로그 헤더 사용자 맞춤화, 116 페이지의 내용을 참조하십시오.
- 템플릿을 생성하여 메시지 본문을 사용자 맞춤화합니다. 시스템 로그 메시지 본문 사용자 맞춤화, 115 페이지의 내용을 참조하십시오.
- 시스템 로그 클라이언트를 구성할 때 ISE에서 미리 정의한 메시지 템플릿을 구문 분석용으로 사용하는 메시지 템플릿으로 사용하거나, 이러한 사전 정의 템플릿에서 사용자 맞춤화한 헤더나 본문 템플릿을 기반으로 사용합니다. 시스템 로그 사전 사전 정의 메시지 템플릿을 이용한 작업, 120 페이지의 내용을 참조하십시오.

시스템 로그 클라이언트 구성

Cisco ISE가 특정 클라이언트에서 시스템 로그 메시지를 수신하게 하려면, 먼저 Cisco ISE에서 특정 클라이언를 정의해야 합니다. 여러 IP 주소를 사용하여 여러 공급자를 정의할 수 있습니다.

시작하기 전에

시작하기 전에 Passive ID(패시브 ID) 및 pxGrid 서비스를 활성화해야 합니다. 자세한 내용은 초기 설정 및 컨피그레이션, 86 페이지를 참고하십시오.

단계 **1** **Work Centers(**작업 센터**)** > **PassiveID(**패시브 **ID)** > **Providers(**제공자**)**를 선택하고 왼쪽 패널에서 **Syslog Providers(**시스템 로그 제공자**)**를 선택합니다.
각 기존 클라이언트에 관한 상태 정보를 포함하는 Syslog Providers(시스템 로그 제공자) 표가 표시됩니다.

단계 **2** 새 시스템 로그 클라이언트를 구성하려면 표 상단에 있는 **Add(**추가**)**를 클릭합니다.

단계 **3** 모든 필수 필드를 작성하고(자세한 내용은 시스템 로그 설정, 110 페이지 항목 참조) 필요하다면 메시지 템플릿을 생성하여(자세한 내용은 시스템 로그 메시지 본문 사용자 맞춤화, 115 페이지 항목 참조) 클라이언트를 올바르게 구성합니다.

단계 **4** **Submit(**제출**)**을 클릭합니다.

시스템 로그 설정

특정 클라이언트가 보내는 시스템 로그 메시지를 이용해 사용자 IDMAC 주소 포함)를 수신하도록 Cisco ISE를 구성합니다. 여러 IP 주소를 사용하여 여러 공급자를 정의할 수 있습니다.

표 ***26: Syslog Providers(***시스템 로그 제공자***)***

필드 이름	설명
Name(이름**)**	구성한 클라이언트를 빠르고 쉽게 구분할 수 있는 고유한 이름을 입력합니다.
Description(설명**)**	이 시스템 로그 제공자에 대한 유의미한 설명입니다.
Status(상태**)**	**Enabled(**활성**)**를 선택하면 구성 완료와 동시에 클라이언트를 활성화합니다.
Host(호스트**)**	호스트 머신의 FQDN을 입력합니다.

필드 이름	설명
Connection Type(연결 유형**)**	UDP 또는 TCP를 입력하여 ISE가 시스템 로그 메시지를 수신 대기하는 채널을 표시합니다. 참고 TCP가 구성된 연결 유형이며 메시지 헤더에 문제가 있어 호스트 이름을 구문 분석할 수 없다면, Cisco ISE는 패킷에서 수신한 IP 주소를 Cisco ISE의 Syslog(시스템 로그) 메시지에 구성된 제공자 목록에 있는 IP 주소와 일치시킵니다. 이 목록을 보려면 **Work Centers(**작업 센터**)** > **PassiveID(**패시브 **ID)** > **Providers(**제공자**)** > **Syslog Providers(**시스템 로그 제공자**)** 를 선택합니다. 구문 분석 성공을 보장하려면 메시지 헤더를 확인하고 필요하다면 사용자 맞춤화하는 것이 좋습니다. 헤더 사용자 맞춤화에 관한 자세한 내용은 시스템 로그 헤더 사용자 맞춤화, 116 페이지 항목을 참조하십시오.

필드 이름	설명
Template(템플릿**)**	

필드 이름	설명
	템플릿은 구문 분석하고, 매핑하고, 전달해야 하는 시스템 로그 메시지 내 정보 부분을 구문 분석기가 식별할 수 있도록 정확한 본문 메시지 구조를 표시합니다. 예를 들어 템플릿은 구문 분석기가 모든 수신 메시지에서 사용자 이름을 찾을 수 있도록, 사용자 이름의 정확한 위치를 표시할 수 있습니다. 이 필드에는 시스템 로그 메시지를 인식하고 올바르게 구문 분석하는 데 사용할 (시스템 로그 메시지 본문용) 템플릿을 표시합니다. 사전 정의된 드롭다운 목록에서 선택하거나 **New(**새로 만들기**)**를 클릭하여 맞춤형 템플릿을 생성합니다. 템플릿 생성에 관한 자세한 내용은 시스템 로그 메시지 본문 사용자 맞춤화, 115 페이지 항목을 참조하십시오. 대부분의 사전 정의 템플릿은 정규식을 사용하며, 맞춤형 템플릿은 반드시 정규식을 사용해야 합니다. 참고 맞춤형 템플릿만 수정하거나 제거할 수 있으며, 드롭다운에 있는 사전 정의된 시스템 템플릿은 수정할 수 없습니다. ISE는 현재 다음과 같은 사전 정의된 DHCP 제공자 템플릿을 제공합니다. • InfoBlox • BlueCat • Lucent_QIP • DHCPD • MSAD DHCP 참고 DHCP 시스템 로그 메시지에는 사용자 이름이 포함되지 않습니다. 따라서 이러한 메시지는 구문 분석기에서 바로 전달되지 않으며, ISE는 올바른 구문 분석과 사용자 ID 정보 전달을 위해 (Live Sessionss(라이브 세션)에 표시되는) 로컬 세션 디렉토리에 등록된 사용자를 먼저 확인한 다음 해당 사용자의 IP 주소를 수신된 DHCP 시스템 로그 메시지에 나열된 IP 주소와 일치시킬 수 있습

필드 이름	설명
	니다. DHCP 시스템 로그 메시지에서 수신한 데이터를 현재 로그인한 사용자 중 누구와도 일치시킬 수 없다면, 메시지는 구문 분석되지 않고 사용자 ID가 전달되지 않습니다. Cisco ISE는 다음과 같은 사전 정의된 일반 시스템 로그 제공자 템플릿을 제공합니다. • ISE • ACS • F5_VPN • ASA_VPN • Blue Coat • Aerohive • Safe connect_NAC • Nortel_VPN 템플릿에 관한 자세한 내용은 시스템 로그 사전 사전 정의 메시지 템플릿을 이용한 작업, 120 페이지 항목을 참조하십시오.
Default Domain(기본 도메인)	도메인이 특정 사용자의 시스템 로그 메시지에서 식별되지 않으면, 모든 사용자에게 도메인이 할당될 수 있도록 이 기본 도메인이 사용자에게 자동으로 할당됩니다. 기본 도메인이나 메시지에서 구문 분석한 도메인을 이용해, 사용자 이름은 username@domain 형식이 되며 사용자 및 사용자 그룹 관련 추가 정보를 얻을 수 있도록 해당 도메인을 포함합니다.

시스템 로그 메시지 구조 사용자 맞춤화(템플릿)

템플릿은 구문 분석하고, 매핑하고, 전달해야 하는 시스템 로그 메시지 내 정보 부분을 구문 분석기가 식별할 수 있도록 정확한 메시지 구조를 표시합니다. 예를 들어 템플릿은 구문 분석기가 모든 수신 메시지에서 사용자 이름을 찾을 수 있도록, 사용자 이름의 정확한 위치를 표시할 수 있습니다. 템플릿은 신규 및 제거 매핑 메시지 모두에서 지원되는 구조를 결정합니다.

Cisco ISE에서는 패시브 ID 구문 분석기에서 사용할 단일 메시지 헤더 및 여러 본문 구조를 사용자 맞춤화할 수 있습니다.

패시브 ID 구문 분석기가 사용자 ID 매핑 추가 메시지인지 제거 메시지인지를 정확하게 식별하고 사용자 세부정보를 올바르게 구문 분석하려면, 템플릿은 사용자 이름, IP 주소, MAC 주소와 도메인의 구조를 정의하는 정규식을 포함해야 합니다.

메시지 템플릿을 사용자 맞춤화할 때 사전 정의된 옵션 내에서 사용되는 정규식 및 메시지 구조를 참조하여 ISE-PIC ISE에 미리 정의된 메시지 템플릿을 기반으로 사용자 맞춤화를 수행할 수 있습니다. 사전 정의된 템플릿 정규식, 메시지 구조, 예제 등에 대한 자세한 내용은 시스템 로그 사전 사전 정의 메시지 템플릿을 이용한 작업, 120 페이지을 참조하십시오.

다음을 사용자 맞춤화할 수 있습니다.

- 단일 메시지 헤더—시스템 로그 헤더 사용자 맞춤화, 116 페이지
- 복수 메시지 본문—시스템 로그 메시지 본문 사용자 맞춤화, 115 페이지

참고 DHCP 시스템 로그 메시지에는 사용자 이름이 포함되지 않습니다. 따라서 이러한 메시지는 구문 분석기에서 바로 전달되지 않으며, ISE는 올바른 구문 분석과 사용자 ID 정보 전달을 위해 (Live Sessionss(라이브 세션)에 표시되는) 로컬 세션 디렉토리에 등록된 사용자를 먼저 확인한 다음 해당 사용자의 IP 주소를 수신된 DHCP 시스템 로그 메시지에 나열된 IP 주소와 일치시킬 수 있습니다. DHCP 시스템 로그 메시지에서 수신한 데이터를 현재 로그인한 사용자 중 누구와도 일치시킬 수 없다면, 메시지는 구문 분석되지 않고 사용자 ID가 전달되지 않습니다.

DHCP 메시지를 올바르게 일치, 구문 분석 및 매핑하는 데 필요한 지연은 사용자 맞춤화 템플릿에는 적용되지 않으며, 따라서 DHCP 메시지 템플릿 사용자 맞춤화은 권장하지 않습니다. 대신 사전 정의된 DHCP 템플릿 중 하나를 사용하십시오.

시스템 로그 메시지 본문 사용자 맞춤화

Cisco ISE를 이용하면 (메시지 본문을 사용자 맞춤화하여) 자체 시스템 로그 메시지 템플릿을 패시브 ID 구문 분석기로 구문 분석하도록 사용자 맞춤화할 수 있습니다. 템플릿에는 사용자 이름, IP 주소, MAC 주소 및 도메인의 구조를 정의하는 정규식이 포함되어야 합니다.

참고 DHCP 시스템 로그 메시지에는 사용자 이름이 포함되지 않습니다. 따라서 이러한 메시지는 구문 분석기에서 바로 전달되지 않으며, Cisco ISE는 올바른 구문 분석과 사용자 ID 정보 전달을 위해 (Live Sessionss(라이브 세션)에 표시되는) 로컬 세션 디렉토리에 등록된 사용자를 먼저 확인한 다음, IP 주소를 기준으로 사용자를 수신한 DHCP 시스템 로그 메시지에 나열된 IP 주소와 일치시킬 수 있습니다. DHCP 시스템 로그 메시지에서 수신한 데이터를 현재 로그인한 사용자 중 누구와도 일치시킬 수 없다면, 메시지는 구문 분석되지 않고 사용자 ID가 전달되지 않습니다.

DHCP 메시지를 올바르게 일치, 구문 분석 및 매핑하는 데 필요한 지연은 사용자 맞춤화 템플릿에는 적용되지 않으며, 따라서 DHCP 메시지 템플릿 사용자 맞춤화은 권장하지 않습니다. 대신 사전 정의된 DHCP 템플릿 중 하나를 사용하십시오.

시스템 로그 클라이언트 구성 화면에서 시스템 로그 메시지 본문 템플릿을 생성하고 수정합니다.

참고 본인의 사용자 맞춤화 템플릿만 수정할 수 있습니다. 시스템에서 제공하는 사전 정의된 템플릿은 수정할 수 없습니다.

단계 1 **Work Centers**(작업 센터) > **PassiveID**(패시브 ID) > **Providers**(제공자)를 선택하고 왼쪽 패널에서 **Syslog Providers**(시스템 로그 제공자)를 선택합니다.
각 기존 클라이언트에 관한 상태 정보를 포함하는 Syslog Providers(시스템 로그 제공자) 표가 표시됩니다.

단계 2 **Add**(추가)를 클릭하여 새 시스템 로그 클라이언트를 추가 하거나 **Edit**(수정)을 클릭하여 이미 구성된 클라이언트를 업데이트합니다. 시스템 로그 클라이언트 구성 및 업데이트에 관한 자세한 내용은 시스템 로그 클라이언트 구성, 109 페이지를 참조하십시오.

단계 3 **Syslog Providers**(시스템 로그 제공자) 창에서 **New**(새로 만들기)를 클릭하여 새 메시지 템플릿을 생성합니다. 기존 템플릿을 수정하려면 드롭다운 목록에서 템플릿을 선택하고 **Edit**(수정)를 클릭합니다.

단계 4 모든 필수 필드를 작성합니다.

올바른 값을 입력하는 자세한 방법은 시스템 로그 맞춤형 템플릿 설정 및 예시, 117 페이지 항목을 참조하십시오.

단계 5 **Test**(테스트)를 클릭하여, 입력된 문자열을 바탕으로 메시지가 올바르게 구문 분석되었는지 확인합니다.

단계 6 **Save**(저장)를 클릭합니다.

시스템 로그 헤더 사용자 맞춤화

시스템 로그 헤더에는 메시지가 생성된 호스트 이름도 포함됩니다. 시스템 로그 메시지를 Cisco ISE 메시지 구문 분석기가 인식하지 못한다면, 호스트 이름 앞에 오는 구분 기호를 구성하여 메시지 헤더를 사용자 맞춤화해야 Cisco ISE가 호스트 이름을 인식하고 메시지를 올바르게 구문 분석할 수 있습니다. 이 화면의 필드에 관한 자세한 내용은 시스템 로그 맞춤형 템플릿 설정 및 예시, 117 페이지 항목을 참조하십시오. 사용자 맞춤화 헤더 구성이 저장되며, 메시지가 수신될 때마다 구문 분석기에서 사용하는 헤더 유형에 추가됩니다.

참고 헤더 하나만 사용자 맞춤화할 수 있습니다. 헤더를 사용자 맞춤화한 후 **Custom Header**(사용자 맞춤화 헤더)를 클릭하고 템플릿을 생성하면 최신 구성만 저장됩니다.

단계 1 **Work Centers**(작업 센터) > **PassiveID**(패시브 ID) > **Providers**(제공자)를 선택하고 왼쪽 패널에서 **Syslog Providers**(시스템 로그 제공자)를 선택합니다.
각 기존 클라이언트에 관한 상태 정보를 포함하는 Syslog Providers(시스템 로그 제공자) 표가 표시됩니다.

단계 2 **Custom Header**(사용자 맞춤화 헤더)를 클릭하여 Syslog Custom Header(시스템 로그 사용자 맞춤화 헤더)를 엽니다.

단계 3 **Paste sample syslog**(시스템 로그 예 붙여넣기)에 시스템 로그 메시지의 헤더 형식 예를 입력합니다. 예를 들어 다음 메시지 중 하나에서 이 헤더를 복사하여 붙여넣습니다. **< 181 > Oct 10 15:14:08 Cisco.com**

단계 **4** **Separator(**구분자**)** 필드에서 단어를 공백과 탭 중 무엇으로 구분할지를 지정합니다.

단계 **5** **Position of hostname in header(**헤더 내 호스트 이름 위치**)**필드에서 호스트 이름 내 헤더 위치를 지정합니다. 예를 들어 위의 헤더에서 호스트 이름은 헤더의 네 번째 단어입니다. 4를 입력하여 이를 표시합니다.

Hostname(호스트 이름**)** 필드는 처음 3개 필드에 표시된 세부정보를 기반으로 호스트 이름을 표시합니다. 예를 들어 **Paste sample syslog(**시스템 로그 예 붙여넣기**)**의 헤더 예가 다음과 같다면

<181>Oct 10 15:14:08 Cisco.com

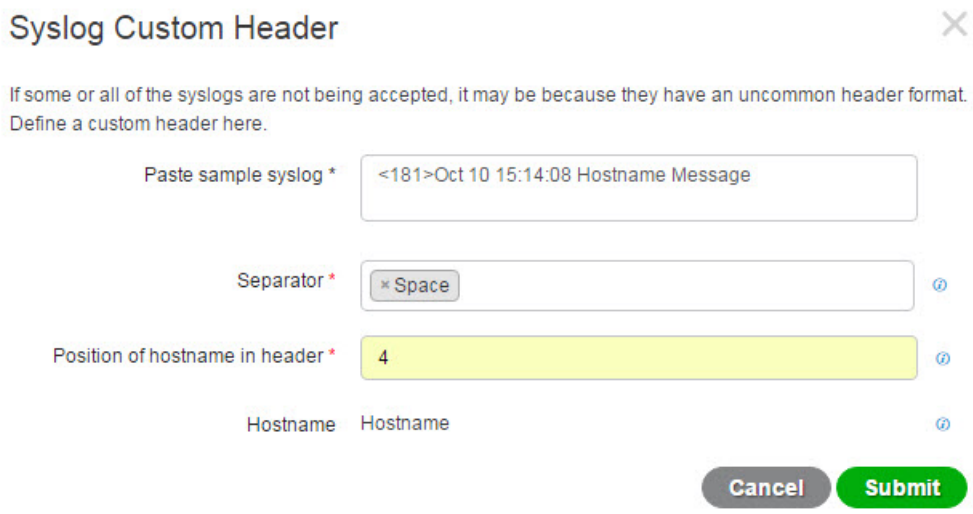
구분 기호는 공백으로 표시되며 헤더 내 호스트 이름 위치는 4로 입력됩니다.

Hostname(호스트 이름**)**은 **Paste sample syslog(**시스템 로그 예 붙여넣기**)** 필드에 붙여넣인 헤더 문구의 네 번째 단어인 Cisco.com으로 자동으로 표시됩니다.

호스트 이름이 잘못 표시된다면 **Seperator(**구분자**)** 및 **(Position of hostname in header(**헤더 내 호스트 이름 위치**)** 필드에 입력한 데이터를 확인하십시오.

이 예시는 다음 화면 캡처처럼 표시됩니다.

그림 ***12:*** 시스템 로그 헤더 사용자 맞춤화



단계 **6** **Submit(**제출**)**을 클릭합니다.
사용자 맞춤화 헤더 구성이 저장되며, 메시지가 수신될 때마다 구문 분석기에서 사용하는 헤더 유형에 추가됩니다.

시스템 로그 맞춤형 템플릿 설정 및 예시

Cisco ISE를 이용하면 자체 시스템 로그 메시지 템플릿을 패시브 ID 구문 분석기로 구문 분석하도록 사용자 맞춤화할 수 있습니다. 맞춤형 템플릿은 신규 및 제거 매핑 메시지 모두에서 지원되는 구조를 결정합니다. 패시브 ID 구문 분석기가 사용자 ID 매핑 추가 메시지인지 제거 메시지인지를 정확하게 식별하고 사용자 세부정보를 올바르게 구문 분석하려면, 템플릿은 사용자 이름, IP 주소, MAC 주소와 도메인의 구조를 정의하는 정규식을 포함해야 합니다.

참고 대부분의 사전 정의된 템플릿은 정규식을 사용합니다. 맞춤형 템플릿은 정규식을 사용해야 합니다.

시스템 로그 헤더 부분

호스트 이름 앞에 오는 구분 기호를 구성하면 시스템 로그 프로브에서 인식하는 단일 헤더를 사용자 맞춤화할 수 있습니다.

다음 표에서는 맞춤형 시스템 로그 헤더에 포함될 수 있는 다양한 부분 및 필드를 설명합니다. 정규식에 관한 자세한 내용은 표 29: 맞춤형 템플릿용 정규식, 120 페이지 항목을 참고하십시오.

표 ***27:*** 시스템 로그 맞춤형 헤더

필드	설명
샘플 시스템 로그 붙여넣기	시스템 로그 메시지에 헤더 형식 예를 입력합니다. 예를 들어 이 헤더를 복사하여 붙여넣습니다. **<181>Oct 10 15:14:08** 호스트 이름 메시지
구분자	단어가 공백과 탭 중 무엇으로 구분되는지를 나타냅니다.
헤더 내 호스트 이름 위치	헤더 내 호스트 위치를 표시합니다. 예를 들어 위의 헤더에서 호스트 이름은 헤더의 네 번째 단어입니다. 4를 입력하여 이를 표시합니다.
호스트 이름	처음 3개 필드에 표시된 세부정보를 기반으로 호스트 이름을 표시합니다. 예를 들어 샘플 시스템 로그 붙여넣기에 있는 헤더 예가 다음과 같다면 <181>Oct 10 15:14:08 호스트 이름 메시지 구분 기호는 공백으로 표시되며 헤더 내 호스트 이름 위치는 4로 입력됩니다. 호스트 이름은 자동으로 Hostname으로 표시됩니다. 호스트 이름이 잘못 표시된다면 구분자 및 헤더 내 호스트 이름 위치 필드에 입력한 데이터를 확인하십시오.

메시지 본문에 대한 시스템 로그 템플릿 부분 및 설명

다음 표에서는 맞춤형 시스템 로그 메시지 템플릿에 포함될 수 있는 다양한 부분 및 필드를 설명합니다. 정규식에 관한 자세한 내용은 표 29: 맞춤형 템플릿용 정규식, 120 페이지 항목을 참고하십시오.

표 ***28:*** 시스템 로그 템플릿

부분	필드	설명
	Name(이름)	이 템플릿의 용도를 인식하는 데 사용하는 고유한 이름입니다.
매핑 작업	새 매핑	새 사용자를 추가하기 위해 이 템플릿과 함께 사용하는 매핑 유형을 설명하는 정규식입니다. 예를 들어 F5 VPN에 로그인한 새 사용자를 나타내려면 이 필드에 'logged on from'을 입력합니다.
	제거된 매핑	사용자를 제거하기 위해 이 템플릿과 함께 사용하는 매핑 유형을 설명하는 정규식입니다. 예를 들어 ASA VPN에서 제거해야 하는 사용자를 나타내려면 이 필드에 'session disconnect'를 입력합니다.
사용자 데이터	IP 주소	캡처할 IP 주소를 나타내는 정규식입니다. 예를 들어 Bluecat 메시지의 경우 이 IP 주소 범위 내에서 사용자 ID를 캡처하려면 다음을 입력합니다. (on\s|to\s)((?:(?:25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\.){3}(?:25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?))
	사용자 이름	캡처할 사용자 이름 형식을 나타내는 정규식입니다.
	도메인	캡처할 도메인을 나타내는 정규식입니다.
	MAC 주소	캡처할 MAC 주소 형식을 나타내는 정규식입니다.

정규식 예

메시지 구문 분석에는 정규식을 사용합니다. 이 섹션에서는 IP 주소, 사용자 이름 및 매핑 추가 메시지를 구문 분석하는 정규식 예를 확인할 수 있습니다.

예를 들어 정규식을 사용하여 다음 메시지를 구문 분석할 수 있습니다.

<174>192.168.0.1 %ASA-4-722051: 그룹 <DfltGrpPolicy> 사용자 <user1> IP <192.168.0.10> IPv4 ㅈ주소 <192.168.0.6> IPv6 주소 <::> 세션에 할당됨

<174>192.168.0.1 %ASA-6-713228: 그룹 = xyz, 사용자 이름 = user1, IP = 192.168.0.12, 할당된 비공개 IP 주소 192.168.0.8 사용자 제거용

정규식은 다음 표에서처럼 정의됩니다.

표 ***29:*** 맞춤형 템플릿용 정규식

부분	정규식
IP 주소	주소 <([^\s]+)>|address ([^\s]+)
사용자 이름	사용자 <([^\s]+)>| 사용자 이름 = ([^\s]+)
매핑 메시지 추가	(%ASA-4-722051|%ASA-6-713228)

시스템 로그 사전 사전 정의 메시지 템플릿을 이용한 작업

시스템 로그 메시지에는 헤더와 메시지 본문을 포함하는 표준 구조가 적용됩니다.

이 섹션에서는 Cisco ISE에서 제공하는 사전 정의 템플릿을 설명하며, 메시지 출처에 따라 지원되는 헤더용 콘텐츠 세부정보와 지원되는 본문 구조도 함께 설명합니다.

또한 시스템에서 사전 정의하지 않은 소스에 대한 맞춤형 본문 콘텐츠를 이용해 자체 템플릿을 만들 수도 있습니다. 이 섹션에서는 맞춤형 템플릿에 지원되는 구조에 대해서도 설명합니다. 메시지를 구문 분석할 때 시스템에 사전 정의된 헤더와 함께 사용할 단일 맞춤형 헤더를 구성할 수 있으며, 메시지 본문용으로 여러 맞춤형 템플릿을 구성할 수 있습니다. 헤더 사용자 맞춤화에 관한 자세한 내용은 시스템 로그 헤더 사용자 맞춤화, 116 페이지 항목을 참조하십시오. 본문 사용자 맞춤화에 관한 자세한 내용은 시스템 로그 메시지 본문 사용자 맞춤화, 115 페이지 항목을 참조하십시오.

참고 대부분의 사전 정의 템플릿은 정규식을 사용하며, 맞춤형 템플릿은 반드시 정규식을 사용해야 합니다.

메시지 헤더

모든 클라이언트 머신의 모든 메시지 유형에 대해, 구문 분석기는 두 가지 헤더 유형(신규 및 제거)을 인식합니다. 두 헤더는 다음과 같습니다.

- <171>호스트 메시지
- <171>Oct 10 15:14:08 호스트 메시지

수신된 헤더는 호스트 이름에 대해 구문 분석됩니다. IP 주소, 호스트 이름 또는 전체 FQDN이 될 수 있습니다.

헤더를 사용자 맞춤화할 수도 있습니다. 헤더를 사용자 맞춤화하는 방법은 시스템 로그 헤더 사용자 맞춤화, 116 페이지 항목을 참조하십시오.

시스템 로그 **ASA VPN** 사전 정의 템플릿

ASA VPN에 대해 지원되는 시스템 로그 메시지 형식 및 유형은 다음과 같습니다.

헤더

구문 분석기에서 지원하는 헤더는 시스템 로그 사전 사전 정의 메시지 템플릿을 이용한 작업, 120 페이지에 설명된 것처럼 모든 클라이언트에서 동일합니다.

새 매핑 본문 메시지

다음 표에 나온 대로 구문 분석기가 인식하는 다양한 ASA VPN 본문 메시지가 있습니다.

본문 메시지	구문 분석 예
%ASA-6-109005 Authentication succeeded for user UserA from 10.0.0.11/100 to 10.10.11.11/20 on interface eth1/1	[UserA,10.0.0.11]
%ASA-6-602303 IPSEC: An direction tunnel_type SA (SPI=spi) between local_IP and 10.0.0.11 (UserA) has been created.	
%ASA-6-721016 (device) WebVPN session for client user UserA, IP 10.0.0.11 has been created.	
%ASA-6-603104 PPTP Tunnel created, tunnel_id is number, remote_peer_ip is remote_address, ppp_virtual_interface_id is number,\ client_dynamic_ip is 10.0.0.11,ffg123 #% UserA is UserA, MPPE_key_strength is string	
%ASA-6-603106 L2TP Tunnel created, tunnel_id is number, remote_peer_ip is remote_address, ppp_virtual_interface_id is number,\ client_dynamic_ip is 10.0.0.11, UserA is user	
%ASA-6-113039 Group group User UserA IP 10.0.0.11 AnyConnect parent session started.	
%ASA-6-802001 User UserA IP 10.100.1.1 OS os_name UDID number MDM action session started.	
%ASA-6-713228: Group = xyz, UserA = xxxx227, IP = 192.168.0.11, Assigned private IP address 172.16.0.11 to remote user	[UserA,172.16.0.11] 참고 이 메시지 유형의 구문 분석된 IP 주소는 메시지에 표시된 대로 개인 IP 주소입니다.
%ASA-4-722051: Group <DfltGrpPolicy> User <UserA> IP <172.16.0.12> IPv4 Address <172.16.0.21> IPv6 address <::> assigned to session	[UserA,172.16.0.12] 참고 이 메시지 유형의 구문 분석된 IP 주소는 IPv4 주소입니다.

매핑 제거 본문 메시지

구문 분석기에서 ASA VPN에 대해 지원하는 매핑 제거 메시지는 이 섹션에 설명되어 있습니다.

본문은 수신된 후에 다음과 같이 사용자 상세정보에 대해 구문 분석됩니다.

[UserA,10.1.1.1]

본문 메시지
%ASA-4-113019 Group = group, UserA = UserA, IP = 10.1.1.1, Session disconnected. Session Type: type, Duration:\ duration, Bytes xmt: count,Bytes rcv: count, Reason: reason
%ASA-4-717052 Group group name User UserA IP 10.1.1.1 Session disconnected due to periodic certificate authentication failure. Subject Name id subject name Issuer Name id issuer name\ Serial Number id serial number
%ASA-6-602304 IPSEC: An direction tunnel_type SA (SPI=spi) between local_IP and 10.1.1.1 (UserA) has been deleted.
%ASA-6-721018 WebVPN session for client user UserA, IP 10.1.1.1 has been deleted.
%ASA-4-722049 Group group User UserA IP 10.1.1.1 Session terminated: SVC not enabled or invalid image on the ASA
%ASA-4-722050 Group group User UserA IP 10.1.1.1 Session terminated: SVC not enabled for the user.
%ASA-6-802002 User UserA IP 10.1.1.1 OS os_name UDID number MDM action session terminated.
%ASA-3-716057 Group group User UserA IP 10.1.1.1 Session terminated, no type license available.
%ASA-3-722046 Group group User UserA IP 10.1.1.1 Session terminated: unable to establish tunnel.
%ASA-4-113035 Group group User UserA IP 10.1.1.1 Session terminated: AnyConnect not enabled or invalid AnyConnect image on the ASA.
%ASA-4-716052 Group group-name User UserA IP 10.1.1.1 Pending session terminated.
%ASA-6-721018 WebVPN session for client user UserA, IP 10.1.1.1 has been deleted.

시스템 로그 **Bluecat** 사전 정의 템플릿

Bluecat에서 지원되는 시스템 로그 메시지 형식 및 유형은 다음과 같습니다.

헤더

구문 분석기에서 지원하는 헤더는 시스템 로그 사전 사전 정의 메시지 템플릿을 이용한 작업, 120 페이지에 설명된 것처럼 모든 클라이언트에서 동일합니다.

새 매핑 본문 메시지

이 섹션에서 설명한 대로 Bluecat 시스템 로그용 새 매핑에 대해 지원되는 메시지가 나와 있습니다.

본문은 수신된 후에 다음과 같이 사용자 세부정보에 대해 구문 분석됩니다.

[macAddress=nn:xx:nn:ca:xx:nn,ip=172.16.0.12]

본문
Nov 7 23:37:32 xx-campus1 dhcpd: DHCPACK on 172.16.0.13 to nn:xx:nn:ca:xx:nn via 172.16.0.17

매핑 제거 메시지

Bluecat에 대해 알려진 매핑 제거 메시지가 없습니다.

시스템 로그 **F5 VPN** 사전 정의 템플릿

F5 VPN에 대해 지원되는 시스템 로그 메시지 형식 및 유형은 다음과 같습니다.

헤더

구문 분석기에서 지원하는 헤더는 시스템 로그 사전 사전 정의 메시지 템플릿을 이용한 작업, 120 페이지에 설명된 것처럼 모든 클라이언트에서 동일합니다.

새 매핑 본문 메시지

다음 표에 나온 대로 구문 분석기가 인식하는 다양한 F5 VPN 본문 메시지가 있습니다.

본문은 수신된 후에 다음과 같이 사용자 세부정보에 대해 구문 분석됩니다.

[user=UserA,ip=172.16.0.12]

본문
Apr 10 09:33:58 Oct 2 08:28:32 abc.xyz.org security[nnnnn]: [UserA@vendor-abcr] User UserA logged on from 172.16.0.21 to \ 172.16.0.12 Sid = xyz\

매핑 제거 메시지

현재 지원되는 F5 VPN에 대한 제거 메시지가 없습니다.

Syslog Infoblox 사전 정의 템플릿

Infoblox에 대해 지원되는 시스템 로그 메시지 형식 및 유형은 다음과 같습니다.

헤더

구문 분석기에서 지원하는 헤더는 시스템 로그 사전 사전 정의 메시지 템플릿을 이용한 작업, 120 페이지에 설명된 것처럼 모든 클라이언트에서 동일합니다.

새 매핑 본문 메시지

다음 표에 나온 대로 구문 분석기가 인식하는 다양한 ASA VPN 본문 메시지가 있습니다.

본문은 수신된 후에 다음과 같이 사용자 상세정보에 대해 구문 분석됩니다.

[macAddress= nn:xx:xx:xx:nn:nn,ip=10.0.10.100]

본문 메시지
Nov 15 11:37:26 user1-lnx dhcpd[3179]: DHCPACK on 10.0.0.14 to nn:xx:xx:nx:nn:nn (android-df67ddcbb1271593) via eth2 relay 10.0.0.24 lease-duration 3600
Nov 15 11:38:11 user1-lnx dhcpd[3179]: DHCPACK on 172.16.0.18 to nn:xx:xx:xn:nn:nn (DESKTOP-HUDGAAQ) via eth2 relay 172.16.0.13 lease-duration 691200 (RENEW)
Nov 15 11:38:11 192.168.0.12 dhcpd[25595]: DHCPACK to 10.0.0.11 (nn:xx:xx:xn:nn:nx) via eth1

매핑 제거 메시지

본문은 수신된 후에 다음과 같이 사용자 상세정보에 대해 구문 분석됩니다.

- MAC 주소가 포함된 경우:

  [00:0c:29:a2:18:34,10.0.10.100]

- MAC 주소가 포함되지 않은 경우:

  [10.0.10.100]

본문 메시지
07-11-2016 23:37:32 Daemon.Info 10.0.10.2 Jul 12 10:42:26 10.0.10.2 dhcpd[26083]: DHCPEXPIRE 10.0.10.100 has expired
07-11-2016 23:37:32 Daemon.Info 10.0.10.2 Jul 12 10:42:26 10.0.10.2 dhcpd[26083]: DHCPRELEASE of 10.0.10.100 from 00:0c:29:a2:18:34 \ (win10) via eth1 uid 01:00:0c:29:a2:18:34
07-11-2016 23:37:32 Daemon.Info 10.0.10.2 Jul 12 10:42:26 10.0.10.2 dhcpd[25595]: RELEASE on 10.20.31.172 to c0:ce:cd:44:4f:bd

시스템 로그 **Linux DHCPd3** 사전 정의 템플릿

Linux DHCPd3에 대해 지원되는 시스템 로그 메시지 형식 및 유형은 다음과 같습니다.

헤더

구문 분석기에서 지원하는 헤더는 시스템 로그 사전 사전 정의 메시지 템플릿을 이용한 작업, 120 페이지에 설명된 것처럼 모든 클라이언트에서 동일합니다.

새 매핑 메시지

다음 표에 설명된 대로 구문 분석기에서 인식하는 다양한 Linux DHCPd3 본문 메시지가 있습니다.

본문은 수신된 후에 다음과 같이 사용자 상세정보에 대해 구문 분석됩니다.

[macAddress=24:ab:81:ca:f2:72,ip=172.16.0.21]

본문 메시지
Nov 11 23:37:32 dhcpsrv dhcpd: DHCPACK on 10.0.10.100 to 00:0c:29:a2:18:34 (win10) via eth1
Nov 11 23:37:32 dhcpsrv dhcpd: DHCPACK on 10.0.10.100 (00:0c:29:a2:18:34) via eth1

매핑 제거 본문 메시지

이 섹션에서는 구문 분석기에서 Linux DHCPd3에 대해 지원하는 매핑 제거 메시지를 설명합니다.

본문은 수신된 후에 다음과 같이 사용자 상세정보에 대해 구문 분석됩니다.

[00:0c:29:a2:18:34 ,10.0.10.100]

본문 메시지
Nov 11 23:37:32 dhcpsrv dhcpd: DHCPEXPIRE 10.0.10.100 has expired
Nov 11 23:37:32 dhcpsrv dhcpd : DHCPRELEASE of 10.0.10.100 from 00 : 0c : 29 : a2 : 18 : 34 (win10) via eth1

시스템 로그 **MS DHCP** 사전 정의 템플릿

MS DHCP에 대해 지원되는 시스템 로그 메시지 형식 및 유형은 다음과 같습니다.

헤더

구문 분석기에서 지원하는 헤더는 시스템 로그 사전 사전 정의 메시지 템플릿을 이용한 작업, 120 페이지에 설명된 것처럼 모든 클라이언트에서 동일합니다.

새 매핑 본문 메시지

다음 표에 나온 대로 구문 분석기가 인식하는 다양한 MS DHCP 본문 메시지가 있습니다.

구문 분석기는 수신된 데이터에서 쉼표(,)를 검색하여 데이터를 분할한 후 다음 예와 같이 이러한 형식의 메시지를 구문 분석합니다.

[macAddress=000C29912E5D,ip=10.0.10.123]

본문 메시지
Nov 11 23:37:32 10,07/21/16,16:55:22,Assign,10.0.10.123,win10.IDCSPAN.Local,000C29912E5D,,724476048,0,,,,0x4D53465420352E30,MSFT,5.0

매핑 제거 본문 메시지

이 섹션에서는 구문 분석기에서 MH DHCP에 대해 지원하는 매핑 제거 메시지를 설명합니다.

구문 분석기는 수신된 데이터에서 쉼표(,)를 검색하여 데이터를 분할한 후 다음 예와 같이 이러한 형식의 메시지를 구문 분석합니다.

[macAddress=000C29912E5D,ip=10.0.10.123]

본문 메시지
Nov 11 23:37:32 12,07/21/16,16:55:18,Release,10.0.10.123,win10.IDCSPAN.Local,000C29912E5D,,3128563632,\ 0,,,,,,,,,0

시스템 로그 **SafeConnect NAC** 사전 정의 템플릿

SafeConnect NAC에 대해 지원되는 시스템 로그 메시지 형식 및 유형은 다음과 같습니다.

헤더

구문 분석기에서 지원하는 헤더는 시스템 로그 사전 사전 정의 메시지 템플릿을 이용한 작업, 120 페이지에 설명된 것처럼 모든 클라이언트에서 동일합니다.

새 매핑 본문 메시지

다음 표에 나온 대로 구문 분석기가 인식하는 SafeConnect NAC 본문 메시지는 다양합니다.

본문은 수신된 후에 다음과 같이 사용자 세부정보에 대해 구문 분석됩니다.

[user=galindk1i,p=xxxx.xx.xxx.xxd,domain=Resnet-Macs]

본문 메시지
Apr 10 09:33:58 nac Safe*Connect: authenticationResult|xxx.xx.xxx.xxx|xxx.xx.xxx.xxx|UserA|true|Resnet-Macs|TCNJ-Chain|001b63b79018|MAC

매핑 제거 메시지

현재 지원되는 안전 연결에 대한 제거 메시지가 없습니다.

시스템 로그 **Aerohive** 사전 정의 템플릿

Aerohive에서 지원되는 시스템 로그 메시지 형식 및 유형은 다음과 같습니다.

헤더

구문 분석기에서 지원하는 헤더는 시스템 로그 사전 사전 정의 메시지 템플릿을 이용한 작업, 120 페이지에 설명된 것처럼 모든 클라이언트에서 동일합니다.

새 매핑 본문 메시지

다음 표에 나온 대로 구문 분석기가 인식하는 다양한 Aerohive 본문 메시지가 있습니다.

본문에서 구문 분석된 세부정보에는 사용자 이름 및 IP 주소가 포함됩니다. 구문 분석에 사용되는 정규식은 다음 예와 같습니다.

- `New mapping—auth\:`
- `IP—ip ([A-F0-9a-f:.]+)`
- `User name—UserA ([a-zA-Z0-9\_]+)`

본문은 수신된 후에 다음과 같이 사용자 세부정보에 대해 구문 분석됩니다.

[UserA,10.5.50.52]

본문 메시지
2013-04-01 14:06:05 info ah auth: Station 1cab:a7e6:cf7f ip 10.5.50.52 UserA UserA

매핑 제거 메시지

현재 시스템은 Aerohive에서 매핑 제거 메시지를 지원하지 않습니다.

시스템 로그 **Blue Coat** 사전 정의 템플릿 **-** 기본 프록시**,** 프록시 **SG, Squid** 웹 프록시

시스템은 Blue Coat에 대해 다음 메시지 유형을 지원합니다.

- Bluecoat 메인 프록시
- BlueCoat Proxy SG
- BlueCoat Squid 웹 프록시

Bluecat 메시지에서 지원되는 시스템 로그 메시지 형식 및 유형은 다음과 같습니다.

헤더

구문 분석기에서 지원하는 헤더는 시스템 로그 사전 사전 정의 메시지 템플릿을 이용한 작업, 120 페이지에 설명된 것처럼 모든 클라이언트에서 동일합니다.

새 매핑 본문 메시지

다음 표에 나온 대로 구문 분석기가 인식하는 다양한 Blue Coat 본문 메시지가 있습니다.

본문은 수신된 후에 다음과 같이 사용자 세부정보에 대해 구문 분석됩니다.

[UserA, 192.168.10.24]

본문 메시지**(**이 예는 **BlueCoat** 프록시 **SG** 메시지에서 가져온 것임**)**
2016-09-21 23:05:33 58 10.0.0.1 UserA - - PROXIED "none" http://www.example.com/ 200 TCP_MISS GET application/json;charset=UTF-8 http site.api.example.com 80 /apis/v2/scoreboard/header ?rand=1474499133503 - "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/46.0.2486.0 Safari/537.36 Edge/13.10586" 192.168.10.24 7186 708 - "unavailable

다음 표에서는 새 매핑 메시지용으로 클라이언트별로 사용되는 여러 정규 표현식 구조에 대해 설명합니다.

클라이언트	정규 표현식
Bluecoat 메인 프록시	새 매핑 **(TCP_HIT|TCP_MEM){1}** IP **\s(?:(?:[0-9]{1,3}\.){3}[0-9]{1,3}|(?:(?:[a-zA-Z0-9]{1,4}:){1,7}[a-zA-Z0-9]{1,4}))\s** 사용자 이름 **\s\-\s([a-zA-Z0-9_]+)\s\-\s**

클라이언트	정규 표현식
BlueCoat Proxy SG	새 매핑 **(\-\sPROXIED){1}** IP **\s(?:[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3})\s(?:[a-zA-Z0-9]{1,4}:{1,2}){1,7}[a-zA-Z0-9]{1,4}\s([a-zA-Z0-9_]+)\s-** 사용자 이름 **\s[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\s([a-zA-Z0-9_]+)\s\-**
BlueCoat Squid 웹 프록시	새 매핑 **(TCP_HIT|TCP_MEM){1}** IP **\s(?:[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3})\s(?:[a-zA-Z0-9]{1,4}:{1,2}){1,7}[a-zA-Z0-9]{1,4})\sTCP** 사용자 이름 **\s([a-zA-Z0-9\._]+)\s\-\/**

매핑 제거 메시지

매핑 제거 메시지는 Blue Coat 클라이언트에 대해 지원되지만 현재 사용 가능한 예는 없습니다.

다음 표에서는 매핑 제거 메시지용으로 클라이언트별로 사용되는 여러 정규 표현식 구조 예에 대해 설명합니다.

클라이언트	정규 표현식
Bluecoat 메인 프록시	**(TCP_MISS|TCP_NC_MISS){1}**
BlueCoat Proxy SG	현재 사용 가능한 예가 없습니다.
BlueCoat Squid 웹 프록시	**(TCP_MISS|TCP_NC_MISS){1}**

시스템 로그 **ISE** 및 **ACS** 사전 정의 템플릿

ISE 또는 ACS 클라이언트를 수신할 때 구문 분석기에서는 다음 메시지 유형을 받습니다.

- 인증 통과: ISE 또는 ACS에서 사용자를 인증하면 사용자 세부정보를 포함하여 인증에 성공했음을 알리는 암호 인증 메시지가 표시됩니다. 메시지가 구문 분석되고 사용자 세부정보 및 세션 ID가 해당 메시지에서 저장됩니다.
- Accounting start and accounting update messages (new mapping)(계정 관리 시작 및 계정 관리 업데이트 메시지(새 매핑)): 계정 관리 시작 또는 계정 관리 업데이트 메시지는 Pass Authentication(인증 통과) 메시지에서 저장한 사용자 세부 정보 및 세션 ID로 구문 분석되고 사용자가 매핑됩니다.
- Accounting stop (remove mapping)(계정 관리 중지(매핑 제거)): 사용자 매핑이 시스템에서 삭제됩니다.

ISE 및 ACS에서 지원되는 시스템 로그 메시지 형식 및 유형은 다음과 같습니다.

인증 통과 메시지

다음 메시지는 인증 통과에 대해 지원됩니다.

- 헤더

  ```
  <181>Sep 13 10:51:41 Server logTag messageId totalFragments currentFragments message
  ```

  예: <181>Sep 13 10:51:41 Positron CISE_PassiveID 0000005255 1 0 message

- 본문

  Passed-Authentication 000011 1 0 2016-05-09 12:48:11.011 +03:00 0000012435 5200 NOTICE Passed-Authentication: Authentication succeeded, ConfigVersionId=104, Device IP Address=10.0.0.12, DestinationIPAddress=10.0.0.18, DestinationPort=1812, UserA=UserA, Protocol=Radius, RequestLatency=45, NetworkDeviceName=DefaultNetworkDevice, User-Name=UserA, NAS-IP-Address=1.1.1.1, Session-Timeout=90, Calling-Station-ID=, cisco-av-pair=audit-session-id=5

- 구문 분석 예

  사용자 이름 및 세션 ID만 구문 분석됩니다.

  [UserA,5]

계정 관리 시작**/**업데이트**(**새 매핑**)** 메시지

다음 메시지는 새 매핑에 대해 지원됩니다.

- 헤더

  ```
  <181>Sep 13 10:51:41 Server logTag messageId totalFragments currentFragments message
  ```

  예: <181>Sep 13 10:51:41 Positron CISE_PassiveID 0000005255 1 0 message

- 본문

  CISE_RADIUS_Accounting 000011 1 0 2016-05-09 12:53:52.823 +03:00 0000012451 3000 NOTICE Radius-Accounting: RADIUS Accounting start request, ConfigVersionId=104, Device IP Address=10.0.0.12, RequestLatency=12, NetworkDeviceName=DefaultNetworkDevice, User-Name=UserA, NAS-IP-Address=10.0.0.1, Framed-IP-Address=10.0.0.16, Session-Timeout=90, Calling-Station-ID=, Acct-Status-Type=Start, Acct-Session-Id=6, cisco-av-pair=audit-session-id=5

- 구문 분석 예

  구문 분석된 세부정보에는 사용자 이름, 프레임 IP 주소 및 메시지에 포함된 MAC 주소가 포함됩니다.

  [UserA,10.0.0.16]

매핑 제거 메시지

다음 메시지는 매핑 제거에 대해 지원됩니다.

- 헤더

  ```
  <181>Sep 13 10:51:41 Server logTag messageId totalFragments currentFragments message
  ```

예: <181>Sep 13 10:51:41 Positron CISE_PassiveID 0000005255 1 0 message

- 본문

  2016-05-09 12:56:27.274 +03:00 0000012482 3001 NOTICE Radius-Accounting: RADIUS Accounting stop request, ConfigVersionId=104, Device IP Address=10.0.0.17, RequestLatency=13, NetworkDeviceName=DefaultNetworkDevice, User-Name=UserA, NAS-IP-Address=10.0.0.1, Framed-IP-Address=10.0.0.16, Session-Timeout=90, Calling-Station-ID=, Acct-Status-Type=Stop, Acct-Session-Id=104, cisco-av-pair=audit-session-id=5

- 구문 분석 예

  구문 분석된 세부정보에는 사용자 이름, 프레임 IP 주소 및 메시지에 포함된 MAC 주소가 포함됩니다.

  [UserA,10.0.0.16]

시스템 로그 **Lucent QIP** 사전 정의 템플릿

Lucent QIP에 대해 지원되는 시스템 로그 메시지 형식 및 유형은 다음과 같습니다.

헤더

구문 분석기에서 지원하는 헤더는 시스템 로그 사전 사전 정의 메시지 템플릿을 이용한 작업, 120 페이지에 설명된 것처럼 모든 클라이언트에서 동일합니다.

새 매핑 본문 메시지

다음 표에 설명된 대로 구문 분석기에서 인식하는 Lucent QIP 본문 메시지는 다양합니다.

이러한 메시지의 정규식 구조는 다음과 같습니다.

DHCP_GrantLease|:DHCP_RenewLease

본문은 수신된 후에 다음과 같이 사용자 상세정보에 대해 구문 분석됩니다.

[00:0C:29:91:2E:5D,10.0.0.11]

본문 메시지
DHCP:subtype=0:Single:$IGNORE_N$ DHCP_GrantLease: Host=$HOSTNAME$ P=10.0.0.11 MAC=00:0C:29:91:2E:5D
DHCP:subtype=0:Single:$IGNORE_N$ DHCP_RenewLease: Host=$HOSTNAME$ P=10.0.0.11 MAC=00:0C:29:91:2E:5D

매핑 제거 본문 메시지

이러한 메시지의 정규식 구조는 다음과 같습니다.

Delete Lease:|DHCP Auto Release:

본문은 수신된 후에 다음과 같이 사용자 상세정보에 대해 구문 분석됩니다.

[10.0.0.11]

본문 메시지
DHCP:subtype=0:Single:$IGNORE_N$ Delete Lease: IP=10.0.0.11 $IGNORE_N$
DHCP:subtype=0:Single:$IGNORE_N$ DHCP Auto Release: IP=10.0.0.11 $IGNORE_N$

패시브 ID 서비스 필터링

이름 또는 IP 주소를 기준으로 특정 사용자를 필터링할 수 있습니다. 예를 들어 엔드포인트를 이용해 일반 관리자를 지원하고자 엔드포인트에 로그인한 IT 서비스 관리자가 있다면, 관리자 활동을 필터링하여 Live Sessions(라이브 세션)에는 표시하지 않고 관련 엔드포인트의 일반 사용자에게만 표시되게 할 수 있습니다. Live Session(라이브 세션)에는 Mapping Filters(매핑 필터)에 의해 필터링되지 않은 패시브 ID 서비스 구성 요소가 표시됩니다. 필터는 필요한 수만큼 추가할 수 있습니다. 필터 사이에는 "OR" 논리 연산자가 적용됩니다. 두 필드를 모두 단일 필터에서 지정하는 경우에는 이러한 필드 사이에 "AND" 논리 연산자가 적용됩니다.

단계 **1** **Work Centers(**작업 센터**)** > **PassiveID(**패시브 **ID)** > **Providers(**제공자**)**를 선택하고 왼쪽 창에서 **Mapping Filters(**매핑 필터**)**를 선택합니다.

단계 **2** **Providers(**제공자**)** > **Mapping Filters(**매핑 필터**)**를 선택합니다.

단계 **3** **Add(**추가**)**를 클릭하고 필터링할 사용자의 사용자 이름 및/또는 IP 주소를 입력한 후에 **Submit(**제출**)**을 클릭합니다.

단계 **4** 현재 모니터링 세션 디렉토리에 로그인되어 있는 필터링되지 않은 사용자를 확인하려면 **Operations(**운영**)** > **RADIUS Livelog(RADIUS** 라이브 로그**)**를 선택합니다.

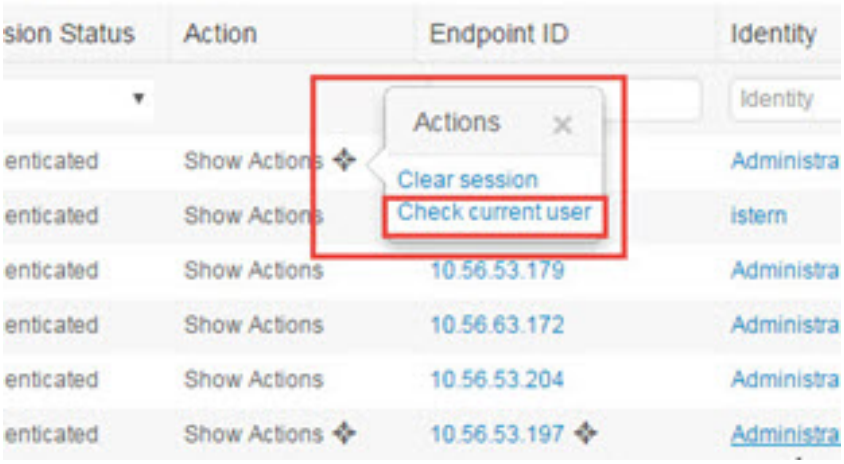
엔드포인트 프로브

사용자가 구성할 수 있는 맞춤형 제공자에 더해, ISE에서 활성화되도록 엔드포인트 프로브를 구성할 수도 있습니다. 단 설치 시 기본적으로 패시브 ID 서비스가 백그라운드에서 항상 실행되어야 합니다. 엔드포인트 프로브는 각 사용자가 여전히 시스템에 로그인해 있는지를 주기적으로 확인합니다.

참고 엔드포인트가 백그라운드에서 실행되게 하려면 먼저 초기 Active Directory 조인 포인트를 구성하고 **Store Credentials(**자격 증명 저장**)**을 선택해야 합니다. 엔드포인트 프로브 구성에 관한 자세한 내용은 엔드포인트 프로브 이용, 132 페이지 항목을 참조하십시오.

엔드포인트 상태를 수동으로 확인하려면 다음 그림에서처럼 **Live Sessions(**라이브 세션**)**로 이동한 다음 **Actions(**작업**)** 열에서 **Show Actions(**작업 표시**)**를 클릭하고 **Check current user(**현재 사용자 확인**)**를 선택합니다.

그림 *13:* 현재 사용자 확인



엔드포인트 사용자 상태에 관한 자세한 정보와 확인을 수동으로 실시하는 방법은 RADIUS 라이브 세션 항목을 참조하십시오.

엔드포인트 프로브가 사용자가 연결되었음을 인식했고 특정 엔드포인트에 대한 세션이 업데이트된 후 4시간이 지났다면, 엔드포인트 프로브는 사용자가 아직도 로그인한 상태인지 확인하고 다음 데이터를 수집합니다.

- MAC 주소
- 운영체제 버전

확인 결과에 따라 프로브는 다음 작업을 수행합니다.

- 사용자가 여전히 로그인된 상태라면 프로브는 Cisco ISE를 Active User(활성 사용자)로 업데이트합니다.
- 사용자가 로그아웃했다면 세션 상태는 Terminated(종료됨)으로 업데이트되며, 15분이 지나면 사용자는 Session Directory에서 제거됩니다.
- 예를 들어 사용자에게 연락할 수 없을 때 방화벽에서 연결을 차단하거나 엔드포인트가 종료된다면, 상태는 Unreachable(연결 불가)로 업데이트되고 Subscriber(가입자) 정책에 따라 사용자 세션 처리 방법이 결정됩니다. 엔드포인트는 여전히 Session Directory에 남습니다.

엔드포인트 프로브 이용

시작하기 전에

서브넷 범위를 기반으로 엔드포인트 프로브를 생성하고 활성화합니다. PSN별로 엔드포인트 프로브 1개를 생성할 수 있습니다. 엔드포인트 프로브를 사용하려면 먼저 다음 항목을 구성했는지 확인해야 합니다.

- 엔드포인트는 포트 445에 네트워크로 연결되어야 합니다.

- ISE에서 초기 Active Directory 조인 포인트를 구성하고, 프롬프트가 표시되면 **Select Credentials(**자격 증명 선택**)**을 선택합니다. 조인 포인트에 관한 자세한 내용은 프로브 및 제공자로서의 Active Directory, 88 페이지 항목을 참조하십시오.

참고 엔드포인트가 백그라운드에서 실행되게 하려면 먼저 Active Directory 프로브를 완전히 구성하지 않은 경우에도 엔드포인트 프로브를 실행할 수 있도록 초기 Active Directory 조인 포인트를 구성해야 합니다.

단계 **1** **Work Centers(**작업 센터**)** > **Passive ID(**패시브 **ID)** > **Providers(**제공자**)**를 선택하고 **Endpoint Probes(**엔드포인트 프로브**)**를 선택합니다.

단계 **2** **Add(**추가**)**를 클릭하여 새 엔드포인트 프로브를 만듭니다.

단계 **3** 필수 필드를 작성합니다. **Status(**상태**)** 필드에서 **Enable(**활성화**)**을 선택하고 **Submit(**제출**)**을 클릭해야 합니다. 자세한 내용은 엔드포인트 프로브 설정, 133 페이지를 참조하십시오.

엔드포인트 프로브 설정

서브넷 범위를 기반으로 PSN별로 엔드포인트 프로브를 하나씩 생성합니다. 구축에 PSN이 여러 개 있다면 각 PSN을 별도의 서브넷 집합에 할당할 수 있습니다.

표 ***30:*** 엔드포인트 프로브 설정

필드 이름	설명
Name(이름**)**	이 프로브 사용 여부를 식별하는 데 사용하는 고유한 이름을 입력합니다.
Description(설명**)**	이 프로브 사용 방법을 설명하는 고유한 설명을 입력합니다.
Status(상태**)**	이 프로브를 활성화하려면 **Enable(**활성화**)**을 선택합니다.
Host Name(호스트 이름**)**	구축에서 사용 가능한 PSN 목록에서 이 프로브의 PSN을 선택합니다.

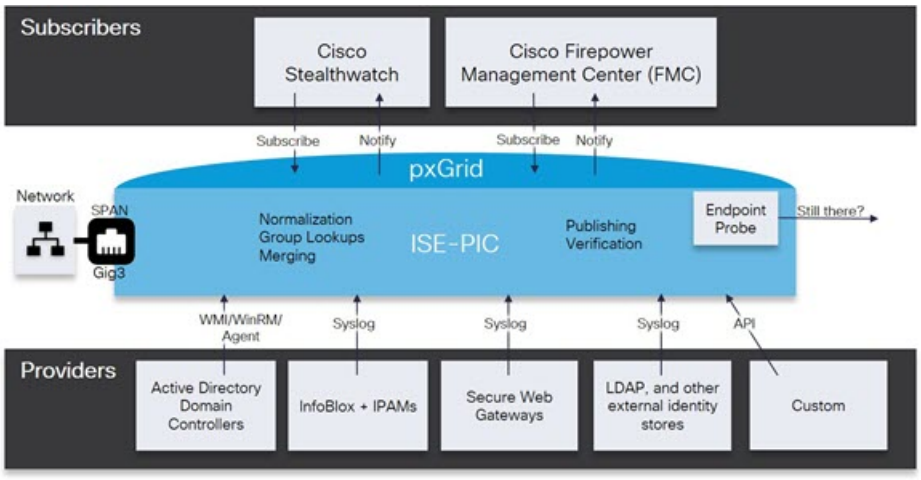
필드 이름	설명
Subnets(서브넷**)**	이 프로브로 확인해야 하는 엔드포인트 그룹의 서브넷 범위를 입력합니다. 표준 서브넷 마스크 범위를 사용하고 쉼표로 서브넷 주소를 구분합니다. 예: 10.56.14.111/32,1.1.1.1/24,2.55.2.0/16,2.2.3.0/16,1.2.3.4/32 각 범위는 고유하며 다른 범위와 구분되어야 합니다. 예를 들어 동일한 프로브에 2.2.2.0/16,2.2.3.0/16을 입력해선 안 됩니다. 서로 겹치는 범위이기 때문입니다.

가입자

패시브 ID 서비스는 Cisco pxGrid 서비스를 사용하여 다양한 제공자로부터 수집하여 Cisco ISE 세션 디렉토리가 저장한 인증된 사용자 ID를 Cisco Stealthwatch나 Cisco FMC(Firepower Management Center) 같은 다른 네트워크 시스템으로 전달합니다.

다음 그림에서 pxGrid 노드는 외부 제공자로부터 사용자 ID를 수집합니다. 이러한 ID는 구문 분석, 매핑 및 형식화됩니다. pxGrid는 형식화된 사용자 ID를 가져와서 패시브 ID 서비스 가입자에게 전송합니다.

그림 ***14:*** 패시브 ***ID*** 서비스 ***Flow***



Cisco ISE에 연결된 가입자는 등록해야 pxGrid 서비스를 사용할 수 있습니다. 가입자는 pxGrid SDK를 통해 Cisco에서 사용 가능한 pxGrid 클라이언트 라이브러리를 채택해야 클라이언트가 될 수 있습니다. 가입자는 고유한 이름과 인증서 기반 상호 인증을 사용하여 pxGrid에 로그인할 수 있습니다. 유효한 인증서를 전송하면, Cisco pxGrid 가입자는 자동으로 ISE에 의해 승인됩니다.

가입자는 pxGrid 서버 호스트 이름 또는 IP 주소에 연결할 수 있습니다. Cisco에서는 불필요한 오류를 방지하기 위해, 특히 DNS 쿼리가 올바르게 작동할 수 있도록 호스트 이름 사용을 권장합니다. 기능

은 가입자가 게시 및 구독할 수 있도록 pxGrid에 생성되는 정보 토픽 또는 채널입니다. Cisco ISE에서는 SessionDirectory 및 IdentityGroup만 지원됩니다. 기능 정보는 **Capabilities(**기능**)** 탭의 **Subscribers(**가입자**)**로 이동하여 게시자로부터 게시, 직접 쿼리 또는 대량 다운로드 쿼리를 통해 사용할 수 있습니다.

가입자가 ISE에서 정보를 수신하게 하려면 다음 작업을 수행해야 합니다.

1. 선택 사항으로, 가입자 측에서 인증서를 생성합니다.
2. PassiveID work center(PassiveID 작업 센터)에서 가입자를 위한 pxGrid 인증서 생성, 135 페이지 작업을 수행합니다.
3. 가입자 활성화, 136 페이지에 전달하는 고성능 고속 어플라이언스입니다. 가입자가 ISE에서 사용자 ID를 수신하게 하려면 이 단계를 수행하거나 승인을 자동으로 활성화해야 합니다. 가입자 설정 구성, 137 페이지의 내용을 참조하십시오.

참고 Cisco ISE 릴리스 3.1부터 모든 pxGrid 연결은 pxGrid 2.0을 기반으로 해야 합니다. pxGrid 1.0 기반(XMPP 기반) 통합은 릴리스 3.1부터 Cisco ISE에서 작동하지 않습니다.

WebSockets를 기반으로 하는 pxGrid 버전 2.0은 Cisco ISE 릴리즈 2.4에서 소개되었습니다. 잠재적인 통합 중단을 방지하려면 다른 시스템을 pxGrid 2.0 호환 버전으로 계획 및 업그레이드하는 것이 좋습니다.

가입자를 위한 **pxGrid** 인증서 생성

시작하기 전에

pxGrid 가입자용 인증서를 생성하여 pxGrid와 가입자 간의 상호 신뢰를 보장하고, 그에 따라 사용자 ID가 ISE에서 가입자로 전달되게 할 수 있습니다. 다음 작업을 수행하려면 슈퍼 관리자 또는 시스템 관리자여야 합니다.

단계 **1** **Work Centers(**작업 센터**)** > **PassiveID(**패시브 **ID)** > **Subscribers(**가입자**)**를 선택하고 **Certificates(**인증서**)** 탭으로 이동합니다.

단계 **2** **I want to(**수행할 작업**)** 드롭다운 목록에서 다음 옵션 중 하나를 선택합니다.

- **Generate a single certificate without a certificate signing request(**인증서 서명 요청 없이 단일 인증서 생성**)**: 이 옵션을 선택하면 CN(Common Name)을 입력해야 합니다. Common Name(일반 이름) 필드에 pxGrid FQDN을 입력합니다(pxGrid는 접두사로 추가됩니다). (예: www.pxgrid-ise.ise.net) 와일드카드를 사용할 수도 있습니다. (예: *. ise.net)
- **Generate a single certificate with a certificate signing request(**인증서 서명 요청을 사용하여 단일 인증서 생성**)**: 이 옵션을 선택하면 인증서 서명 요청 세부정보를 입력해야 합니다.
- **Generate bulk certificates(**대량 인증서 생성**)**: 필수 세부정보를 포함하는 CSV 파일을 업로드할 수 있습니다.

- **Download Root Certificate Chain(**루트 인증서 체인 다운로드**)**: ISE 공용 루트 인증서를 다운로드하여 pxGrid 클라이언트의 신뢰할 수 있는 인증서 저장소에 추가합니다. ISE pxGrid 노드는 새로 서명한 pxGrid 클라이언트 인증서만 신뢰하며 반대의 경우도 마찬가지라, 외부 인증 기관을 이용하지 않아도 됩니다.

단계 **3** (선택 사항) 이 인증서에 대한 설명을 입력합니다.

단계 **4** 이 인증서가 기반으로 하는 pxGrid 인증서 템플릿을 보거나 수정합니다. 인증서 템플릿은 해당 템플릿을 기준으로 CA(Certificate Authority)에서 발급한 모든 인증서에 일반적인 속성을 포함합니다. 인증서 템플릿은 사용해야 하는 주체, SAN(Subject Alternative Name), 키 크기, SCEP RA 프로파일, 인증서의 유효 기간, 그리고 클라이언트 또는 서버 인증이나 두 인증에 모두 인증서를 사용해야 하는지 여부를 지정하는 EKU(Extended Key Usage: 확장 키 사용)를 정의합니다. 내부 Cisco ISE CA(ISE CA)는 인증서 템플릿을 사용하여 해당 템플릿을 기준으로 인증서를 발급합니다. 이 템플릿을 수정하려면 **Administration(**관리**)** > **Certificates(**인증서**)** > **Certificate Authority(**인증 기관**)** > **Certificate Templates(**인증서 템플릿**)**를 선택합니다.

단계 **5** SAN(대체 주체 이름)을 지정합니다. 여러 SAN을 추가해도 됩니다. 다음 옵션을 사용할 수 있습니다.

- **FQDN**: ISE 노드의 정규화된 도메인 이름을 입력합니다. (예: www.isepic.ise.net) FQDN에 와일드카드를 사용할 수도 있습니다. (예: *. ise.net)

  pxGrid FQDN을 입력할 수 있는 FQDN용 추가 회선을 추가할 수 있습니다. Common Name(일반 이름) 필드에 사용한 FQDN과 동일해야 합니다.

- **IP address(IP** 주소**)**: 인증서에 연결할 ISE 노드의 IP 주소를 입력합니다. 가입자가 FQDN 대신 IP 주소를 사용한다면 이 정보를 반드시 입력해야 합니다.

참고 Generate Bulk Certificate(대량 인증서 생성) 옵션을 선택했다면 이 필드는 표시되지 않습니다.

단계 **6** **Certificate Download Format(**인증서 다운로드 형식**)** 드롭다운 목록에서 다음 옵션 중 하나를 선택합니다.

- **PEM(Private Enhanced Electronic Mail)** 형식의 인증서**, PKCS8 PEM** 형식의 키**(**인증서 체인 포함**))**: 루트 인증서, 중간 CA 인증서 및 최종 엔티티 인증서는 PEM 형식으로 표시됩니다. PEM 형식 인증서는 BASE64 인코딩 ASCII 파일입니다. 각 인증서는 "--------BEGIN CERTIFICATE-----" 태그로 시작하고 "-------END CERTIFICATE----" 태그로 끝납니다. 최종 엔티티의 개인 키는 PKCS * PEM을 사용하여 저장됩니다. "-----BEGIN ENCRYPTED PRIVATE KEY----" 태그로 시작하고 "-----END ENCRYPTED PRIVATE KEY----" 태그로 끝납니다.

- **PKCS12 format (including certificate chain; one file for both the certificate chain and key)(PKCS12** 형식**(**인증서 체인 포함**,** 인증서 체인과 모두를 위한 단일 파일**))**: 루트 CA 인증서, 중간 CA 인증서, 최종 엔티티의 인증서 및 개인 키를 단일 암호화 파일에 저장하는 이진 형식입니다.

단계 **7** 인증서 비밀번호를 입력합니다.

단계 **8** **Create(**생성**)**를 클릭합니다.

가입자 활성화

가입자가 Cisco ISE에서 사용자 ID를 수신하려면 이 작업을 수행하거나 승인을 자동으로 활성화해야 합니다. 가입자 설정 구성, 137 페이지를 참조하십시오.

시작하기 전에

- Cisco pxGrid 클라이언트에서 요청을 확인하려면 하나 이상의 노드에서 pxGrid 페르소나를 활성화합니다.
- Passive Identity Service를 활성화합니다. 자세한 내용은 Easy Connect, 81 페이지를 참고하십시오.

단계 **1** **Work Centers(**작업 센터**)** > **PassiveID(**패시브 **ID)** > **Subscribers(**가입자**)**를 선택하고 **Clients(**클라이언트**)** 탭이 표시되는지 확인합니다.

단계 **2** 가입자 옆의 확인란을 선택하고 **Approve(**승인**)**를 클릭합니다.

단계 **3** 최신 상태를 보려면 **Refresh(**새로 고침**)**를 클릭합니다.

Live Logs(라이브 로그)에서 가입자 이벤트 보기

Live Logs(라이브 로그) 페이지에는 모든 가입자 이벤트가 표시됩니다. 이벤트 정보에는 이벤트 유형 및 타임스탬프와 함께 가입자 및 기능 이름이 포함됩니다.

Subscribers(가입자**)**로 이동하고 **Live Log(**라이브 로그**)** 탭을 선택하여 이벤트 목록을 확인합니다. 로그를 지우고 목록을 다시 동기화하거나 새로 고칠 수도 있습니다.

가입자 설정 구성

시작하기 전에

다음 작업을 수행하려면 슈퍼 관리자 또는 시스템 관리자여야 합니다.

단계 **1** **Administration(**관리**)** > **pxGrid Services(pxGrid** 서비스**)** > **Settings(**설정**)**를 선택합니다.

단계 **2** 요건에 따라 다음 옵션을 선택합니다.

- **Automatically Approve New Accounts(**새 계정 자동 승인**)**: 새 pxGrid 클라이언트의 연결 요청을 자동으로 승인하려면 이 확인란을 선택합니다.
- **Allow Password Based Account Creation(**암호 기반 계정 생성 허용**)**: pxGrid 클라이언트에 대해 사용자 이름/암호 기반 인증을 활성화하려면 이 확인란을 선택합니다. 이 옵션을 활성화하면 pxGrid 클라이언트를 자동으로 승인할 수 없습니다.

  pxGrid 클라이언트는 REST API를 통해 사용자 이름을 전송하여 pxGrid 컨트롤러에 자체적으로 등록할 수 있습니다. pxGrid 컨트롤러는 클라이언트 등록 중에 pxGrid 클라이언트의 비밀번호를 생성합니다. 관리자는 연결 요청을 승인하거나 거부할 수 있습니다.

단계 **3** **Save(**저장**)**를 클릭합니다.

PassiveID Work Center(패시브 ID 작업 센터)에서의 모니터링 및 문제 해결 PassiveID 작업 센터

이 섹션에서는 모니터링, 문제 해결 및 보고 도구를 사용하여 PassiveID 작업 센터를 관리하는 .

- *Cisco ISE* 관리 가이드*:* 문제 해결의 RADIUS 라이브 세션 섹션을 참조하십시오.
- *Cisco ISE* 관리 가이드*:* 문제 해결의 Cisco ISE 경보 섹션을 참조하십시오.
- *Cisco ISE* 관리 가이드*:* 유지 관리 및 모니터링의 보고서 섹션을 참조하십시오.
- *Cisco ISE* 관리 가이드*:* 문제 해결의 들어오는 트래픽을 검증하는 TCP 덤프 유틸리티 섹션을 참조하십시오.

LDAP

LDAP(Lightweight Directory Access Protocol)는 RFC 2251에 정의된 네트워킹 프로토콜로, TCP/IP를 기반으로 실행되는 디렉토리 서비스를 쿼리하고 수정할 수 있습니다. LDAP는 X.500 기반 디렉토리 서버에 액세스하는 데 사용되는 경량 메커니즘입니다.

Cisco ISE는 LDAP 프로토콜을 사용하여 ID 소스라고도 하는 LDAP 외부 데이터베이스에 통합됩니다.

LDAP 디렉토리 서비스

LDAP 디렉토리 서비스는 클라이언트 서버 모델을 기반으로 합니다. 클라이언트는 LDAP 서버를 연결하고 작업 요청을 서버에 보내어 LDAP 세션을 시작합니다. 그런 다음 서버는 응답을 보냅니다. 하나 이상의 LDAP 서버에는 LDAP 디렉토리 트리 또는 LDAP 백엔드 데이터베이스의 데이터가 있습니다.

디렉토리 서비스는 정보가 포함된 데이터베이스에 해당하는 디렉토리를 관리합니다. 디렉토리 서비스는 정보를 저장하기 위해 분산형 모델을 사용하며 정보는 일반적으로 디렉토리 서버 간에 복제됩니다.

LDAP 디렉토리는 단순 트리 계층으로 구성되며 여러 서버 간에 분산될 수 있습니다. 각 서버에는 전체 디렉토리의 복제된 버전이 있을 수 있으며 이는 정기적으로 동기화됩니다.

트리 항목에는 속성 집합이 있으며, 각 속성에는 이름(속성 유형 또는 속성 설명)과 하나 이상의 값이 있습니다. 속성은 스키마로 정의됩니다.

각 항목에는 고유 식별자, 즉 DN(Distinguished Name)이 있습니다. 이 이름에는 항목의 속성과 상위 항목의 DN으로 구성된 RDN(Relative Distinguished Name)이 있습니다. DN을 전체 파일 이름으로, RDN을 폴더의 상대 파일 이름으로 간주할 수 있습니다.

여러 LDAP 인스턴스

서로 다른 IP 주소 또는 포트 설정을 사용하여 여러 LDAP 인스턴스를 생성하면 여러 LDAP 서버 또는 동일한 LDAP 서버의 여러 데이터베이스를 사용하여 인증하도록 Cisco ISE를 구성할 수 있습니다. 각각의 기본 서버 IP 주소 및 포트 컨피그레이션은 보조 서버 IP 주소 및 포트 컨피그레이션과 함께 하나의 Cisco ISE LDAP ID 소스 인스턴스에 해당하는 LDAP 인스턴스를 형성합니다.

Cisco ISE에서 각 LDAP 인스턴스가 고유한 LDAP 데이터베이스에 해당할 필요는 없습니다. 동일한 데이터베이스에 액세스하기 위해 여러 LDAP 인스턴스를 설정할 수 있습니다. 이 방법은 LDAP 데이터베이스에 사용자 또는 그룹의 서브트리가 여러 개 있는 경우에 유용합니다. 각 LDAP 인스턴스는 사용자와 그룹마다 각각 하나의 서브트리 디렉토리만 지원하므로 Cisco ISE가 인증 요청을 제출하는 각 사용자 디렉토리 및 그룹 디렉토리 서브트리 조합에 대해 별도의 LDAP 인스턴스를 구성해야 합니다.

LDAP 페일오버

Cisco ISE는 기본 LDAP 서버와 보조 LDAP 서버 간 페일오버를 지원합니다. 작동 중지되었거나 연결할 수 없는 이유로 Cisco ISE가 LDAP 서버에 연결할 수 없기 때문에 인증 요청에 실패하는 경우에 페일오버가 발생합니다.

페일오버를 설정한 상태에서 Cisco ISE가 연결하려고 하는 첫 번째 LDAP 서버에 연결할 수 없는 경우 Cisco ISE는 항상 두 번째 LDAP 서버에 연결하려고 시도합니다. Cisco ISE에서 첫 번째 LDAP 서버를 다시 사용하게 하려면 장애 복구 재시도 지연(Failback Retry Delay) 텍스트 상자에 값을 입력해야 합니다.

참고 Cisco ISE는 항상 기본 LDAP 서버를 사용하여 관리 포털에서 권한 부여 정책에 사용할 그룹 및 속성을 가져옵니다. 따라서 이러한 항목을 구성하는 경우 기본 LDAP 서버에 액세스할 수 있어야 합니다. Cisco ISE는 페일오버 컨피그레이션에 따라 런타임에 인증 및 권한 부여를 위해서만 보조 LDAP 서버를 사용합니다.

LDAP 연결 관리

Cisco ISE는 여러 동시 LDAP 연결을 지원합니다. 연결은 처음 LDAP 인증하는 시점에 온디맨드 방식으로 열립니다. 각 LDAP 서버마다 최대 연결 수가 구성되어 있습니다. 연결을 미리 열면 인증 시간이 단축됩니다. 동시 바인딩 연결에 사용할 최대 연결 수를 설정할 수 있습니다. 열린 연결 수는 각 LDAP 서버(기본 또는 보조)마다 다를 수 있으며 각 서버에 구성된 최대 관리 연결 수에 따라 결정됩니다.

Cisco ISE에는 Cisco ISE에 구성된 각 LDAP 서버의 열린 LDAP 연결 목록(바인딩 정보 포함)이 있습니다. 인증 프로세스 중에 연결 관리자는 풀에서 열린 연결을 찾으려고 합니다. 열린 연결이 없으면 새 연결이 열립니다.

LDAP 서버에서 연결이 닫히면 연결 관리자는 디렉토리를 검색하기 위한 첫 번째 호출 중에 오류를 보고하고 연결을 다시 시작하려고 시도합니다. 인증 프로세스가 완료되면 연결 관리자가 연결을 해제합니다.

LDAP 사용자 인증

LDAP를 외부 ID 저장소로 구성할 수 있습니다. Cisco ISE는 일반 비밀번호 인증을 지원합니다. 사용자 인증에는 다음과 같은 작업이 포함됩니다.

- LDAP 서버에서 요청의 사용자 이름과 일치하는 항목 검색
- LDAP 서버에서 발견된 비밀번호를 사용하여 사용자 비밀번호 확인
- 정책에 사용할 그룹의 멤버십 정보 검색
- 정책 및 권한 부여 프로파일에 사용할 지정된 속성 값 검색

Cisco ISE는 사용자 인증을 위해 바인딩 요청을 LDAP 서버에 보냅니다. 바인딩 요청에는 사용자의 DN 및 비밀번호가 일반 텍스트 형식으로 포함되어 있습니다. 사용자의 DN 및 비밀번호가 LDAP 디렉토리의 사용자 이름 및 비밀번호와 일치하면 사용자가 인증됩니다.

Active Directory가 LDAP로 사용되는 경우 UPN 이름이 사용자 인증에 사용됩니다. Sun ONE Directory Server를 LDAP로 사용하는 경우 SAM 이름이 사용자 인증에 사용됩니다.

참고 Cisco ISE는 모든 사용자 인증에 대해 두 개의 searchRequest 메시지를 전송합니다. 이는 Cisco ISE 권한 부여 또는 네트워크 성능에 영향을 주지 않습니다. 두 번째 LDAP 요청은 Ciso ISE가 올바른 ID와 통신하는지 확인하는 것입니다.

참고 Cisco ISE는 DNS 클라이언트로 DNS 응답에서 반환된 첫 번째 IP만 사용하여 LDAP 바인딩을 수행합니다.

SSL(Secure Sockets Layer)을 사용하여 LDAP 서버 연결을 보호하는 것이 좋습니다.

참고 비밀번호가 만료된 후 계정에 대한 유예 로그인이 남아 있는 경우에만 LDAP에 대한 비밀번호 변경이 지원됩니다. 비밀번호 변경이 성공하면 LDAP 서버의 bindResponse는 LDAP_SUCCESS이며, 나머지 유예 로그인 제어 필드를 bindResponse 메시지에 포함합니다. bindResponse 메시지에 추가 제어 필드(남은 유예 로그인 제외)가 포함되어 있으면 Cisco ISE가 메시지를 디코딩하지 못할 수 있습니다.

권한 부여 정책에 사용할 LDAP 그룹 및 속성 검색

Cisco ISE는 디렉토리 서버에 대해 바인딩 작업을 수행하여 주체를 찾아 인증하는 방식으로 LDAP ID 소스에 대해 주체(사용자 또는 호스트)를 인증할 수 있습니다. 인증에 성공한 후에 Cisco ISE는 필요하면 언제든지 그룹과 함께 주체에 속하는 속성을 검색할 수 있습니다. Cisco ISE 관리 포털에서 **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **External Identity Sources(**외부 **ID** 소스**)** > **LDAP**를 선택하여 검색할 속성을 구성할 수 있습니다. Cisco ISE에서 주체에 권한을 부여하는 데 이러한 그룹 및 속성을 사용할 수 있습니다

사용자를 인증하거나 LDAP ID 소스를 쿼리할 때 Cisco ISE는 LDAP 서버에 연결하고 연결 풀을 유지 관리합니다.

Active Directory를 LDAP 저장소로 구성한 경우 그룹 멤버십에 다음과 같은 제한 사항이 적용됩니다.

- 사용자 또는 컴퓨터는 정책 조건에 정의된 그룹의 직접 멤버여야 정책 규칙과 일치될 수 있습니다.
- 정의된 그룹은 사용자 또는 컴퓨터의 기본 그룹이 아닐 수 있습니다. 이 제한 사항은 Active Directory가 LDAP 저장소로 구성된 경우에만 적용됩니다.

LDAP 그룹 멤버십 정보 검색

사용자 인증, 사용자 조회 및 MAC 주소 조회에서 Cisco ISE는 LDAP 데이터베이스에서 그룹 멤버십 정보를 검색해야 합니다. LDAP 서버는 다음 중 한 가지 방법으로 주체(사용자 또는 호스트)와 그룹 간 연결을 나타냅니다.

- Groups Refer to Subjects(그룹이 주체를 참조함): 그룹 객체에 주체를 지정하는 속성이 포함되어 있습니다. 주체 식별자는 그룹에 다음과 같이 제공될 수 있습니다.
  - 고유 이름
  - 일반 사용자 이름
- Subjects Refer to Groups(주체가 그룹을 참조함): 주체 객체에 객체가 속하는 그룹을 지정하는 속성이 포함되어 있습니다.

LDAP ID 소스에는 그룹 멤버십 정보 검색을 위한 다음 매개변수가 포함되어 있습니다.

- Reference direction: 이 매개변수는 그룹 멤버십을 결정(그룹에서 주체로, 또는 주체에서 그룹으로)할 때 사용할 방법을 지정합니다.
- Group map attribute: 이 매개변수는 그룹 멤버십 정보가 들어 있는 속성을 나타냅니다.
- Group object class: 이 매개변수는 특정 객체가 그룹으로 인식되는지를 결정합니다.
- Group search subtree: 이 매개변수는 그룹 검색을 위한 검색 기준을 나타냅니다.
- Member type option: 이 매개변수는 멤버가 그룹 멤버 속성에 저장되는 방식(DN 또는 일반 사용자 이름으로)을 지정합니다.

LDAP 속성 검색

사용자 인증, 사용자 조회 및 MAC 주소 조회의 경우 Cisco ISE는 LDAP 데이터베이스에서 주체 속성을 검색해야 합니다. 각 LDAP ID 소스 인스턴스마다 ID 소스 사전이 생성됩니다. 이러한 사전은 다음과 같은 데이터 형식의 속성을 지원합니다.

- 문자열
- 서명되지 않은 정수 32
- IPv4 주소

서명되지 않은 정수 및 IPv4 속성의 경우 Cisco ISE는 검색된 문자열을 해당 데이터 형식으로 변환합니다. 변환이 실패하거나 속성 값이 검색되지 않으면 Cisco ISE는 디버깅 메시지를 기록하지만 인증 또는 조회 프로세스는 실패하지 않습니다.

변환이 실패하거나 Cisco ISE에서 속성 값이 검색되지 않으면, Cisco ISE가 사용할 수 있는 속성의 기본값을 선택적으로 구성할 수 있습니다.

LDAP 인증서 검색

사용자 조회의 일부로 인증서 검색을 구성한 경우 Cisco ISE는 LDAP에서 인증서 속성 값을 검색해야 합니다. LDAP에서 인증서 속성 값을 검색하려면 이전에 LDAP ID 소스를 구성하면서 액세스하는 속성 목록에서 인증서 속성을 구성해야 합니다.

LDAP 서버에서 반환하는 오류

인증 프로세스 중에는 다음 오류가 발생할 수 있습니다.

- 인증 오류 - Cisco ISE는 Cisco ISE 로그 파일에 인증 오류를 기록합니다.

  LDAP 서버가 바인딩(인증) 오류를 반환할 수 있는 원인은 다음과 같습니다.

  - 매개변수 오류 - 잘못된 매개변수를 입력했습니다.
  - 사용자 계정이 비활성화되었거나 잠겼거나 만료되었거나 비밀번호가 만료되는 등 계정이 제한되었습니다.
  - 초기화 오류 - LDAP 서버 시간 초과 설정을 사용하여 Cisco ISE가 LDAP 서버의 연결 또는 인증이 실패했다고 결정할 때까지 해당 서버에서 응답을 대기해야 하는 시간(초)을 구성합니다.

    LDAP 서버가 초기화 오류를 반환할 수 있는 이유는 다음과 같습니다.

    - LDAP가 지원되지 않습니다.
    - 서버가 다운되었습니다.
    - 서버의 메모리가 부족합니다.
    - 사용자에게 권한이 없습니다.
    - 관리자 자격 증명이 잘못 구성되었습니다.

LDAP 서버에 문제가 있을 수 있음을 나타내는 다음 오류가 외부 리소스 오류로 기록됩니다.

- 연결 오류가 발생했습니다.
- 시간 초과 기간이 만료되었습니다.
- 서버가 다운되었습니다.
- 서버의 메모리가 부족합니다.

다음 오류는 알 수 없는 사용자 오류로 기록됩니다.

- 사용자가 데이터베이스에 없습니다.

다음 오류는 사용자는 있지만 전송된 비밀번호는 잘못되었음을 나타내는 잘못된 비밀번호 오류로 기록됩니다.

- 잘못된 비밀번호를 입력했습니다.

LDAP 사용자 조회

Cisco ISE는 LDAP 서버를 사용한 사용자 조회 기능을 지원합니다. 이 기능을 사용하면 LDAP 데이터베이스에서 사용자를 검색하고 인증 없이 정보를 찾아올 수 있습니다. 사용자 조회 프로세스에는 다음과 같은 작업이 포함됩니다.

- LDAP 서버에서 요청의 사용자 이름과 일치하는 항목 검색
- 정책에 사용할 사용자의 그룹 멤버십 정보 검색
- 정책 및 권한 부여 프로파일에 사용할 지정된 속성 값 검색

LDAP MAC 주소 조회

Cisco ISE는 MAC 주소 조회 기능을 지원합니다. 이 기능을 사용하면 LDAP 데이터베이스에서 MAC 주소를 검색하고 인증 없이 정보를 찾아올 수 있습니다. MAC 주소 조회 프로세스에는 다음과 같은 작업이 포함됩니다.

- LDAP 서버에서 디바이스의 MAC 주소와 일치하는 항목 검색
- 정책에 사용할 디바이스의 MAC 주소 그룹 정보 검색
- 정책에 사용할 지정된 속성 값 검색

LDAP ID 소스 추가

시작하기 전에

- 다음 작업을 수행하려면 슈퍼 관리자 또는 시스템 관리자여야 합니다.
- Cisco ISE는 항상 기본 LDAP 서버를 사용하여 권한 부여 정책에서 사용할 그룹과 속성을 가져옵니다. 따라서 이러한 항목을 구성할 때 기본 LDAP 서버에 연결할 수 있어야 합니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **External Identity Sources(**외부 **ID** 소스**)** > **LDAP** > **Add(**추가**)**를 선택합니다.

단계 **2** 값을 입력합니다.

단계 **3** **Submit(**제출**)**을 클릭하여 LDAP 인스턴스를 생성합니다.

LDAP ID 소스 설정

다음 표에서는 LDAP 인스턴스를 생성하고 해당 인스턴스에 연결하는 데 사용할 수 있는 LDAP ID 소스 창의 필드에 대해 설명합니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **External Identity Sources(**외부 **ID** 소스**)** > **LDAP**입니다.

LDAP 일반 설정

다음 표에서는 **General(**일반**)** 탭의 필드에 대해 설명합니다.

표 ***31: LDAP*** 일반 설정

필드 이름	사용 지침
Name(이름**)**	LDAP 인스턴스 이름을 입력합니다. 이 값은 검색에서 주체 DN 및 속성을 가져오는 데 사용됩니다. 값은 문자열 유형이며 최대 길이는 64자입니다.
Description(설명**)**	LDAP 인스턴스에 대한 설명을 입력합니다. 이 값은 문자열 유형이며 최대 길이는 1,024자입니다.
Schema(스키마**)**	다음과 같은 내장 스키마 유형 중 하나를 선택하거나 사용자 맞춤화 스키마를 생성할 수 있습니다. • Active Directory • Sun Directory 서버 • Novell eDirectory Schema(스키마) 옆의 화살표를 클릭하여 스키마 세부정보를 확인할 수 있습니다. 사전 정의된 스키마의 속성을 편집하면 Cisco ISE가 자동으로 사용자 맞춤화 스키마를 생성합니다.
참고 다음 필드는 사용자 맞춤화 스키마를 선택할 때만 편집할 수 있습니다.	
Subject Objectclass	검색에서 주체 DN 및 속성을 가져오기 위해 사용할 값을 입력합니다. 값은 문자열 유형이며 최대 길이는 256자입니다.
Subject Name Attribute(주체 이름 속성**)**	요청의 사용자 이름이 포함된 속성의 이름을 입력합니다. 값은 문자열 유형이며 최대 길이는 256자입니다.

필드 이름	사용 지침
Group Name Attribute(그룹 이름 속성**)**	• CN: 공용 이름을 기준으로 LDAP ID 저장소 그룹을 검색하려는 경우 입력합니다. • DN: 고유 이름을 기준으로 LDAP ID 저장소 그룹을 검색하려는 경우 입력합니다.
Certificate Attribute(인증서 속성**)**	인증서 정의를 포함하는 속성을 입력합니다. 인증서 기반 인증의 경우 이러한 정의는 클라이언트가 제공하는 인증서를 검증하는 데 사용됩니다.
Group Objectclass	검색에서 그룹으로 인식되는 객체를 지정하기 위해 사용할 값을 입력합니다. 값은 문자열 유형이며 최대 길이는 256자입니다.
Group Map Attribute(그룹 맵 속성**)**	매핑된 정보를 포함하는 속성을 지정합니다. 이 속성은 선택한 참조 방향에 따라 사용자 또는 그룹 속성일 수 있습니다.
Subject Objects Contain Reference To Groups(주체 객체가 그룹에 대한 참조를 포함함**)**	주체 객체가 속한 그룹을 지정하는 속성이 주체 객체에 포함되어 있으면 이 옵션을 클릭합니다.
Group Objects Contain Reference To Subjects(그룹 객체가 주체에 대한 참조를 포함함**)**	그룹 객체가 주체를 지정하는 속성을 포함하고 있으면 이 옵션을 클릭합니다. 이 값이 기본값입니다.
Subjects in Groups Are Stored in Member Attribute As(그룹의 주체가 멤버 속성에 다른 이름으로 저장됨**)**	(**Group Objects Contain Reference To Subjects(**그룹 객체가 주체에 대한 참조를 포함함**)** 옵션을 활성화하는 경우에만 사용 가능함) 그룹 멤버 속성에서 멤버가 제공되는 방법을 지정하며, 기본값은 DN입니다.

필드 이름	사용 지침
User Info Attributes(사용자 정보 속성**)**	기본적으로, 사전 정의된 속성은 다음과 같은 내장 스키마 유형에 대한 사용자 정보(예: 이름, 성, 이메일, 전화 번호, 소재지 등)를 수집하는 데 사용됩니다. • Active Directory • Sun Directory 서버 • Novell eDirectory 사전 정의된 스키마의 속성을 편집하면 Cisco ISE가 자동으로 사용자 맞춤화 스키마를 생성합니다. 스키마 드롭다운 목록에서 Custom(사용자 맞춤화) 옵션을 선택하여 요건에 따라 사용자 정보 속성을 편집할 수도 있습니다.

LDAP 연결 설정

다음 표에서는 **Connection Settings(**연결 설정**)** 탭의 필드에 대해 설명합니다.

표 ***32: LDAP*** 연결 설정

필드 이름	사용 지침
Enable Secondary Server(보조 서버 활성화**)**	기본 LDAP 서버에서 장애가 발생하는 경우 백업으로 사용할 보조 LDAP 서버를 활성화하려면 이 옵션을 선택합니다. 이 확인란을 선택하는 경우 보조 LDAP 서버에 대한 컨피그레이션 매개변수를 입력해야 합니다.
Primary and Secondary Servers(기본 서버 및 보조 서버**)**	
Hostname/IP(호스트 이름/**IP)**	LDAP 소프트웨어를 실행 중인 머신의 IP 주소 또는 DNS 이름을 입력합니다. 호스트 이름은 1~256자로 입력하거나 문자열로 표시되는 유효한 IP 주소를 포함할 수 있습니다. 호스트 이름에 사용할 수 있는 문자는 영숫자 문자(a~z, A~Z, 0~9)와 점(.), 하이픈(-)입니다.
Port(포트**)**	LDAP 서버가 수신 대기 중인 TCP/IP 포트 번호를 입력합니다. 유효한 값은 1~65,535입니다. 기본값은 LDAP 사양에 나와 있는 389입니다. 포트 번호를 모르는 경우 LDAP 서버 관리자에서 이 정보를 찾을 수 있습니다.

필드 이름	사용 지침
Specify server for each ISE node(각 **ISE** 노드에 대한 서버 지정**)**	각 PSN에 대해 기본 및 보조 LDAP 서버 호스트 이름/IP 및 해당 포트를 구성하려면 이 확인란을 선택합니다. 이 옵션을 활성화하면 구축의 모든 노드를 나열하는 표가 표시됩니다. 노드를 선택하고 선택한 노드에 대한 기본 및 보조 LDAP 서버 호스트 이름/IP 및 해당 포트를 구성해야 합니다.
Access(액세스**)**	**Anonymous Access(**익명 액세스**)**: LDAP 디렉토리의 검색이 익명으로 수행되도록 하려면 클릭합니다. 이 경우 서버는 클라이언트를 구분하지 않으며, 인증되지 않은 클라이언트가 액세스할 수 있도록 구성된 모든 데이터에 대한 읽기 권한을 클라이언트에 허용합니다. 서버로 인증 정보를 전송하도록 허용하는 특정 정책이 없는 경우 클라이언트는 익명 연결을 사용해야 합니다. **Authenticated Access(**인증된 액세스**)**: LDAP 디렉토리의 검색이 관리 자격 증명을 사용하여 수행되도록 하려면 클릭합니다. 이 설정을 클릭하는 경우 Admin DN(관리자 DN) 및 Password(비밀번호) 필드에 정보를 입력합니다.
Admin DN(관리자 **DN)**	관리자의 DN을 입력합니다. 관리자 DN은 사용자 디렉토리 서브트리에서 필요한 모든 사용자 및 그룹을 검색할 권한이 있는 LDAP 계정입니다. 지정된 관리자에게 검색에서 그룹 이름 속성을 확인할 권한이 없으면 해당 LDAP 서버에 의해 인증된 사용자에 대한 그룹 매핑이 실패합니다.
Password(비밀번호**)**	LDAP 관리자 계정 비밀번호를 입력합니다.
Secure Authentication(보안 인증**)**	SSL을 사용하여 Cisco ISE와 기본 LDAP 서버 간의 통신을 암호화하려면 클릭합니다. Port(포트) 필드에 LDAP 서버의 SSL에 사용되는 포트 번호가 포함되어 있는지 확인합니다. 이 옵션을 활성화하는 경우 루트 CA를 선택해야 합니다.
LDAP Server Root CA(LDAP 서버 루트 **CA)**	인증서를 사용한 보안 인증을 활성화하려면 드롭다운 목록에서 신뢰할 수 있는 루트 인증 기관을 선택합니다.

필드 이름	사용 지침
Server Timeout(서버 시간 초과**)**	기본 LDAP 서버와의 연결이나 인증이 실패했다고 결정할 때까지 Cisco ISE가 해당 서버로부터의 응답을 대기할 시간을 초 단위로 입력합니다. 유효한 값은 1~99입니다. 기본값은 10입니다.
Max. Admin Connections(최대 관리자 연결 수**)**	특정 LDAP 컨피그레이션에 대해 실행할 수 있는 LDAP 관리자 계정 권한이 있는 최대 동시 연결 수(0보다 큼)를 입력합니다. 이러한 연결은 디렉토리 검색 시 사용자 디렉토리 서브트리 및 그룹 디렉토리 서브트리에서 사용자와 그룹을 검색하는 데 사용됩니다. 유효한 값은 1~99입니다. 기본값은 20입니다.
Force reconnect every N seconds(N초마다 강제로 다시 연결**)**	서버가 지정된 시간 간격에 LDAP 연결을 갱신하도록 강제 지정하려면 이 확인란을 선택하고 **Seconds(**초**)** 필드에 원하는 값을 입력합니다. 유효 범위는 1분~60분입니다.
Test Bind to Server(서버에 대한 바인딩 테스트**)**	LDAP 서버 세부정보 및 자격 증명을 정상적으로 바인딩할 수 있는지를 테스트하고 확인하려면 클릭합니다. 테스트가 실패하는 경우 LDAP 서버 세부정보를 편집한 후에 다시 테스트해 주십시오.
Failover(페일오버**)**	
Always Access Primary Server First(항상 기본 서버에 먼저 액세스**)**	Cisco ISE가 인증 및 권한 부여를 위해 항상 기본 LDAP 서버에 먼저 액세스하도록 하려면 이 옵션을 클릭합니다.
Failback to Primary Server After(다음 시간 이후 기본 서버로 장애 복구**)**	Cisco ISE가 연결하려고 하는 기본 LDAP 서버에 연결할 수 없는 경우 Cisco ISE는 보조 LDAP 서버에 연결하려고 시도합니다. Cisco ISE가 기본 LDAP 서버를 다시 사용하도록 하려면 이 옵션을 클릭하고 텍스트 상자에 값을 입력합니다.

LDAP 디렉토리 조직 설정

다음 표에서는 **Directory Organization(**디렉토리 조직**)** 탭의 필드에 대해 설명합니다.

표 ***33: LDAP*** 디렉토리 조직 설정

필드 이름	사용 지침
Subject Search Base(주체 검색 기준**)**	모든 주체를 포함하는 서브트리의 DN을 입력합니다. 예를 들면 다음과 같습니다. o=corporation.com 주체를 포함하는 트리가 기본 DN인 경우 LDAP 컨피그레이션에 따라 o=corporation.com 또는 dc=corporation,dc=com 을 입력합니다. 자세한 내용은 LDAP 데이터베이스 설명서를 참고해 주십시오.
Group Search Base(그룹 검색 기준**)**	모든 그룹을 포함하는 서브트리의 DN을 입력합니다. 예를 들면 다음과 같습니다. ou=조직 단위, ou=다음 조직 단위, o=corporation.com 그룹을 포함하는 트리가 기본 DN인 경우 LDAP 컨피그레이션에 따라 o=corporation.com 또는 dc=corporation,dc=com 을 입력합니다. 자세한 내용은 LDAP 데이터베이스 설명서를 참고해 주십시오.

필드 이름	사용 지침
Search for MAC Address in Format(MAC 주소 검색 형식**)**	LDAP 데이터베이스에서 Cisco ISE가 검색에 사용할 MAC 주소 형식을 입력합니다. 내부 ID 소스의 MAC 주소는 xx-xx-xx-xx-xx-xx 형식으로 제공됩니다. LDAP 데이터베이스의 MAC 주소는 다른 형식으로 제공될 수 있습니다. 그러나 Cisco ISE는 호스트 조회 요청을 받으면 MAC 주소를 내부 형식에서 이 필드에 지정된 형식으로 변환합니다. 드롭다운 목록을 사용하여 특정 형식의 MAC 주소 검색을 활성화합니다. 여기서 <*format*>은 다음 중 하나일 수 있습니다. • xxxx.xxxx.xxxx • xxxxxxxxxxxx • xx-xx-xx-xx-xx-xx • xx:xx:xx:xx:xx:xx 선택한 형식은 LDAP 서버에서 제공되는 MAC 주소의 형식과 일치해야 합니다.
Strip Start of Subject Name Up To the Last Occurrence of the Separator(마지막으로 나타나는 구분 기호까지 주체 이름 시작 부분 분리**)**	사용자 이름에서 도메인 접두사를 제거하려면 적절한 텍스트를 입력합니다. Cisco ISE는 사용자 이름에서 이 필드에 지정된 구분 기호 문자를 찾으면 사용자 이름이 시작되는 부분부터 구분 기호 문자까지의 모든 문자를 분리합니다. <start_string> 상자에 지정된 문자 중 두 개 이상이 사용자 이름에 포함되어 있으면 Cisco ISE는 마지막으로 나타나는 구분 기호까지 문자를 분리합니다. 예를 들어 구분 기호 문자가 백슬래시(\)이고 사용자 이름이 DOMAIN\user1이면 Cisco ISE는 user1을 LDAP 서버에 제출합니다. 참고 <start_string>은 우물 정자(#), 물음표(?), 큰따옴표("), 별표(*), 오른쪽 꺾쇠 괄호(>) 및 왼쪽 꺾쇠 괄호(<)와 같은 특수 문자를 포함할 수 없습니다. Cisco ISE에서는 사용자 이름에 이러한 문자를 사용할 수 없습니다.

필드 이름	사용 지침
Strip End of Subject Name from the First Occurrence of the Separator(처음으로 나타나는 구분 기호부터 주체 이름 끝 부분 분리**)**	사용자 이름에서 도메인 접미사를 제거하려면 적절한 텍스트를 입력합니다. Cisco ISE는 사용자 이름에서 이 필드에 지정된 구분 기호 문자를 찾으면 구분 기호 문자부터 사용자 이름이 끝나는 부분까지의 모든 문자를 분리합니다. 이 필드에 지정된 문자 중 두 개 이상이 사용자 이름에 포함되어 있으면 Cisco ISE는 처음으로 나타나는 구분 기호부터 문자를 분리합니다. 예를 들어 구분 기호 문자가 @이고 사용자 이름이 *user1@domain*이면 Cisco ISE는 *user1*을 LDAP 서버에 제출합니다. 참고 <*end_string*> 상자에는 우물 정자(#), 물음표(?), 큰따옴표("), 별표(*), 오른쪽 꺾쇠 괄호(>) 및 왼쪽 꺾쇠 괄호(<)와 같은 특수 문자를 포함할 수 없습니다. Cisco ISE에서는 사용자 이름에 이러한 문자를 사용할 수 없습니다.

LDAP 그룹 설정

표 ***34: LDAP*** 그룹 설정

필드 이름	사용 지침
Add(추가**)**	새 그룹을 추가하려면 **Add(**추가**) > Add Group(**추가 그룹**)**을 선택합니다. 또는 LDAP 디렉토리에서 그룹을 선택하려면 **Add(**추가**) > Select Groups From Directory(**디렉토리에서 그룹 선택**)**를 선택합니다. 그룹을 추가하도록 선택하는 경우 새 그룹의 이름을 입력합니다. 디렉토리에서 선택하는 경우 필터 기준을 입력하고 **Retrieve Groups(**그룹 검색**)**를 클릭합니다. 선택할 그룹 옆의 확인란을 선택하고 **OK(**확인**)**를 클릭합니다. 선택한 그룹이 **Groups(**그룹**)** 창에 표시됩니다.

LDAP 속성 설정

표 *35: LDAP* 속성 설정

필드 이름	사용 지침
Add(추가)	새 속성을 추가하려면 **Add(추가) > Add Attribute(속성 추가)**를 선택합니다. 또는 LDAP 서버에서 속성을 선택하려면 **Add(추가) > Select Attributes From Directory(디렉토리에서 속성 선택)**를 선택합니다. 속성을 추가하도록 선택하는 경우 새 속성의 이름을 입력합니다. 디렉토리에서 선택하는 경우 사용자 이름을 입력하고 **Retrieve Attributes(속성 검색)**를 클릭하여 속성을 검색합니다. 선택할 속성 옆의 확인란을 선택하고 OK(확인)를 클릭합니다.

LDAP 고급 설정

다음 표에서는 Advanced Settings(고급 설정) 탭의 필드에 대해 설명합니다.

표 *36: LDAP* 고급 설정

필드 이름	사용 지침
Enable Password Change(비밀번호 변경 활성화)	디바이스 관리자에 PAP 프로토콜을 사용하고 네트워크 액세스에 RADIUS EAP-GTC 프로토콜을 사용하는 동안 비밀번호 만료 또는 비밀번호 재설정이 발생할 때 사용자가 비밀번호를 변경할 수 있도록하려면 이 확인란을 선택합니다. 지원되지 않는 프로토콜에 대한 사용자 인증은 실패합니다. 또한 이 옵션을 사용하면 사용자가 다음 로그인 시 비밀번호를 변경할 수 있습니다.

관련 항목

LDAP 디렉토리 서비스, 138 페이지
LDAP 사용자 인증, 140 페이지
LDAP 사용자 조회, 143 페이지
LDAP ID 소스 추가, 143 페이지

LDAP 스키마 구성

단계 **1** **Administration(관리) > Identity Management(ID 관리) > External Identity Sources(외부 ID 소스) > LDAP**Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 .

단계 **2** LDAP 인스턴스를 선택합니다.

단계 **3** **General(일반)** 탭을 클릭합니다.

단계 **4** **Schema(스키마)** 옵션 근처의 드롭다운 화살표를 클릭합니다.

단계 **5** **Schema(스키마)** 드롭다운 목록에서 필요한 스키마를 선택합니다. **Custom(사용자 맞춤화)** 옵션을 선택하여 요구 사항에 따라 속성을 업데이트할 수 있습니다.

사전 정의된 속성은 Active Directory, Sun Directory Server, Novell eDirectory와 같은 기본 제공 스키마에 사용됩니다. 사전 정의된 스키마의 속성을 편집하면 Cisco ISE가 자동으로 사용자 맞춤화 스키마를 생성합니다.

기본 및 보조 LDAP 서버 구성

LDAP 인스턴스를 생성한 후에는 기본 LDAP 서버에 대한 연결 설정을 구성해야 합니다. 보조 LDAP 서버는 필요에 따라 구성하면 됩니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **External Identity Sources(**외부 **ID** 소스**)** > **LDAP**를 선택합니다.

단계 **2** 편집할 LDAP 인스턴스 옆의 확인란을 선택하고 **Edit(**편집**)**를 클릭합니다.

단계 **3** **Connection(**연결**)** 탭을 클릭하여 기본 및 보조 서버를 구성합니다.

단계 **4** LDAP ID 소스 설정의 설명에 따라 값을 입력합니다.

단계 **5** **Submit(**제출**)**을 클릭하여 연결 매개변수를 저장합니다.

Cisco ISE가 LDAP 서버에서 속성을 가져오도록 설정

Cisco ISE가 LDAP 서버에서 사용자 및 그룹 데이터를 가져오도록 하려면 Cisco ISE에서 LDAP 디렉토리 세부정보를 구성해야 합니다. LDAP ID 소스에 대해 다음의 세 가지 검색을 수행할 수 있습니다.

- 관리용으로 그룹 서브트리의 모든 그룹 검색
- 사용자를 찾기 위해 주체 서브트리에서 사용자 검색
- 사용자가 멤버로 속한 그룹 검색

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **External Identity Sources(**외부 **ID** 소스**)** > **LDAP**를 선택합니다.

단계 **2** 편집할 LDAP 인스턴스 옆의 확인란을 선택하고 **Edit(**편집**)**를 클릭합니다.

단계 **3** **Directory Organization(**디렉토리 구성**)** 탭을 클릭합니다.

단계 **4** LDAP ID 소스 설정의 설명에 따라 값을 입력합니다.

단계 **5** 컨피그레이션을 저장하려면 **Submit(**제출**)**을 클릭합니다.

LDAP 서버에서 그룹 멤버십 세부정보 검색

새 그룹을 추가하거나 LDAP 디렉토리에서 그룹을 선택할 수 있습니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **External Identity Sources(**외부 **ID** 소스**)** > **LDAP**를 선택합니다.

단계 2 편집할 LDAP 인스턴스 옆의 확인란을 선택하고 **Edit(**편집**)**를 클릭합니다.

단계 3 **Groups(**그룹**)** 탭을 클릭합니다.

단계 4 **Add(**추가**)** > **Add Group(**그룹 추가**)**을 선택하여 새 그룹을 추가하거나 **Add(**추가**)** > **Select Groups From Directory(**디렉토리에서 그룹 선택**)**를 선택하여 LDAP 디렉토리에서 그룹을 선택합니다.

a) 그룹을 추가하도록 선택하는 경우 새 그룹의 이름을 입력합니다.

b) 디렉토리에서 선택하는 경우 필터 기준을 입력하고 **Retrieve Groups(**그룹 검색**)**를 클릭합니다. 검색 조건에는 별표(*) 와일드카드 문자를 포함할 수 있습니다.

단계 5 선택할 그룹 옆의 확인란을 선택하고 **OK(**확인**)**를 클릭합니다.

선택한 그룹이 그룹 페이지에 표시됩니다.

단계 6 **Submit(**제출**)**을 클릭하여 그룹 선택 사항을 저장합니다.

참고 Active Directory가 Cisco ISE에서 LDAP ID 저장소로 구성되어 있으면 Active Directory 내장 그룹은 지원되지 않습니다.

LDAP 서버에서 사용자 속성 검색

권한 부여 정책에서 사용할 사용자 속성을 LDAP 서버에서 가져올 수 있습니다.

단계 1 **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **External Identity Sources(**외부 **ID** 소스**)** > **LDAP**를 선택합니다.

단계 2 편집할 LDAP 인스턴스 옆의 확인란을 선택하고 **Edit(**편집**)**를 클릭합니다.

단계 3 **Attributes(**속성**)** 탭을 클릭합니다.

단계 4 새 속성을 추가하려면 **Add(**추가**)** > **Add Attribute(**속성 추가**)**를 선택합니다. 또는 LDAP 서버에서 속성을 선택하려면 **Add(**추가**)** > **Select Attributes From Directory(**디렉토리에서 속성 선택**)**를 선택합니다.

a) 속성을 추가하도록 선택하는 경우 새 속성의 이름을 입력합니다.

b) 디렉토리에서 선택하는 경우 예제 사용자를 입력하고 **Retrieve Attributes(**속성 검색**)**를 클릭하여 사용자 속성을 검색합니다. 별표(*) 와일드카드 문자를 사용할 수 있습니다.

Cisco ISE에서는 속성 유형 IP를 수동으로 추가할 때 사용자 인증에 IPv4 또는 IPv6 주소를 사용하도록 LDAP 서버를 구성할 수 있습니다.

단계 5 선택할 속성 옆의 확인란을 선택하고 **OK(**확인**)**를 클릭합니다.

단계 6 **Submit(**제출**)**을 클릭하여 속성 선택 사항을 저장합니다.

LDAP ID 소스를 사용한 보안 인증 활성화

LDAP 컨피그레이션 페이지의 Secure Authentication(보안 인증) 옵션을 선택하면 Cisco ISE는 SSL을 사용하여 LDAP ID 소스와의 통신을 보호합니다. LDAP ID 소스에 대한 보안 연결은 다음 항목을 사용하여 설정됩니다.

- SSL 터널: SSL v3 또는 TLS v1(LDAP 서버에서 지원하는 가장 강력한 버전)을 사용합니다.
- 서버 인증(LDAP 서버의 인증): 인증서를 기반으로 합니다.
- 클라이언트 인증(Cisco ISE의 인증): 사용되지 않습니다. SSL 터널 내부에서 관리자 바인딩이 사용됩니다.
- 암호 세트: Cisco ISE에서 지원하는 모든 암호 세트가 사용됩니다.

Cisco ISE가 지원하는 가장 강력한 암호화 및 암호를 제공하는 TLS v1을 사용하는 것이 좋습니다.

Cisco ISE가 LDAP ID 소스와 안전하게 통신할 수 있도록 설정하려면 다음을 수행합니다.

시작하기 전에

- Cisco ISE를 LDAP 서버에 연결해야 합니다.
- TCP 포트 636를 열어야 합니다.

단계 **1** LDAP 서버에 서버 인증서를 발급한 CA(Certificate Authority)의 전체 CA 체인을 Cisco ISE(**Administration(**관리**)** > **System(**시스템**)** > **Certificates(**인증서**)** > **Trusted Certificates(**신뢰할 수 있는 인증서**)**)로 가져옵니다.

전체 CA 체인은 LDAP 서버 인증서가 아닌 루트 CA 및 중간 CA 인증서를 참고합니다.

단계 **2** LDAP ID 소스와 통신할 때 보안 인증을 사용하도록 Cisco ISE를 구성합니다(**Administration(**관리**)** > **Identity Management(ID** 관리**)** > **External Identity Sources(**외부 **ID** 소스**)** > **LDAP**). 이때 Connection Settings(연결 설정) 탭에서 Secure Authentication(보안 인증) 확인란을 선택해야 합니다.

단계 **3** LDAP ID 저장소의 루트 CA 인증서를 선택합니다.

ODBC ID 소스

ODBC(Open Database Connectivity) 준수 데이터베이스를 외부 ID 소스로 사용하여 사용자와 엔드포인트를 인증할 수 있습니다. ODBC ID 소스는 ID 저장소 시퀀스에서, 그리고 게스트 및 스폰서 인증용으로 사용할 수 있습니다. 또한 BYOD 플로우에도 사용할 수 있습니다.

다음 데이터베이스 엔진이 지원됩니다.

- MySQL
- Oracle
- PostgreSQL

- Microsoft SQL Server
- Sybase

ODBC 준수 데이터베이스에 대해 인증하도록 Cisco ISE를 구성해도 데이터베이스 컨피그레이션에는 영향을 주지 않습니다. 데이터베이스를 관리하려면 데이터베이스 설명서를 참고하십시오.

참고 Cisco ISE는 ODBC를 사용한 암호화를 지원하지 않습니다. 따라서 ODBC 연결은 보호되지 않습니다.

ODBC 데이터베이스의 자격 증명 확인

Cisco ISE는 ODBC 데이터베이스에 대해 각기 다른 3가지 유형의 자격 증명 확인을 지원합니다. 각 자격 증명 확인 유형에 대해 적절한 SQL 저장 프로시저를 구성해야 합니다. Cisco ISE는 이 저장 프로시저를 이용해 ODBC 데이터베이스에서 적절한 표를 쿼리하고 ODBC 데이터베이스에서 출력 파라미터 또는 기록 집합을 수신합니다. 데이터베이스는 ODBC 쿼리에 대한 응답으로 기록 집합 또는 명명된 파라미터 집합을 반환할 수 있습니다.

비밀번호는 일반 텍스트 또는 암호화된 형식으로 ODBC 데이터베이스에 저장할 수 있습니다. 저장 절차는 Cisco ISE에서 호출될 때 비밀번호를 일반 텍스트로 다시 암호 해독할 수 있습니다.

자격 증명 확인 유형	**ODBC** 입력 파라미터	**ODBC** 출력 파라미터	자격 증명 확인	인증 프로토콜
ODBC 데이터베이스의 일반 텍스트 비밀번호 인증	사용자 이름 비밀번호	결과 그룹 계정 정보 오류 문자열	사용자 이름과 비밀번호가 일치하는 경우 관련 사용자 정보가 반환됩니다.	PAP EAP-GTC(PEAP 또는 EAP-FAST의 내부 방법) TACACS
ODBC 데이터베이스에서 가져오는 일반 텍스트 비밀번호	사용자 이름	결과 그룹 계정 정보 오류 문자열 비밀번호	사용자 이름이 있는 경우 해당 비밀번호와 관련 사용자 정보가 저장 절차에 의해 반환됩니다. Cisco ISE는 인증 방법에 근거해 비밀번호 해시를 계산한 다음 이를 클라이언트에서 수신한 비밀번호와 비교합니다.	CHAP MSCHAPv1/v2 EAP-MD5 LEAP EAP-MSCHAPv2(PEAP 또는 EAP-FAST의 내부 방법) TACACS

자격 증명 확인 유형	ODBC 입력 파라미터	ODBC 출력 파라미터	자격 증명 확인	인증 프로토콜
조회	사용자 이름	결과 그룹 계정 정보 오류 문자열	사용자 이름이 있는 경우 관련 사용자 정보가 반환됩니다.	MAB PEAP, EAP-FAST 및 EAP-TTLS의 빠른 재연결

참고 ODBC가 권한 부여를 위한 조회 소스로 사용되는 경우, ODBC 데이터베이스와 수신 요청 MAB 형식이 동일한지 확인하십시오.

출력 파라미터에서 반환되는 그룹은 Cisco ISE에서 사용되지 않습니다. Fetch Groups(그룹 가져오기) 저장 절차에 의해 검색된 그룹만 Cisco ISE에서 사용됩니다. 계정 정보는 인증 감사 로그에만 포함됩니다.

다음 표에는 ODBC 데이터베이스 저장 프로시저에서 반환되는 결과 코드와 Cisco ISE 인증 결과 코드 간의 매핑이 나열되어 있습니다.

결과 코드(저장 프로시저에 의해 반환됨)	설명	Cisco ISE 인증 결과 코드
0	CODE_SUCCESS	NA(인증 통과됨)
1	CODE_UNKNOWN_USER	UnknownUser
2	CODE_INVALID_PASSWORD	Failed
3	CODE_UNKNOWN_USER_OR_INVALID_PASSWORD	UnknownUser
4	CODE_INTERNAL_ERROR	Error
10001	CODE_ACCOUNT_DISABLED	DisabledUser
10002	CODE_PASSWORD_EXPIRED	NotPerformedPasswordExpired

참고 Cisco ISE는 이 매핑된 인증 결과 코드를 기반으로 실제 인증 또는 조회 작업을 수행합니다.

저장 절차를 사용하여 ODBC 데이터베이스에서 그룹 및 속성을 가져올 수 있습니다.

일반 텍스트 비밀번호 인증용 기록 집합을 반환하는 샘플 절차(**Microsoft SQL Server**용)

```
CREATE PROCEDURE [dbo].[ISEAuthUserPlainReturnsRecordset]
        @username varchar(64), @password varchar(255)
AS
BEGIN
```

```
        IF EXISTS( SELECT  username
        FROM  NetworkUsers
        WHERE  username  = @username
        AND  password  = @password )
        SELECT 0,11,'give full access','No Error'
        FROM  NetworkUsers
        WHERE  username  = @username
        ELSE
        SELECT 3,0,'odbc','ODBC Authen Error'
END
```

일반 텍스트 비밀번호 가져오기용 기록 집합을 반환하는 샘플 절차(Microsoft SQL Server용)

```
CREATE PROCEDURE [dbo].[ISEFetchPasswordReturnsRecordset]
        @username varchar(64)
AS
BEGIN
        IF EXISTS( SELECT  username
        FROM  NetworkUsers
        WHERE  username  = @username)
        SELECT 0,11,'give full access','No Error',password
        FROM  NetworkUsers
        WHERE  username  = @username
        ELSE
        SELECT 3,0,'odbc','ODBC Authen Error'
END
```

조회용 기록 집합을 반환하는 샘플 절차(Microsoft SQL Server용)

```
CREATE PROCEDURE [dbo].[ISEUserLookupReturnsRecordset]
        @username varchar(64)
AS
BEGIN
        IF EXISTS( SELECT  username
        FROM  NetworkUsers
        WHERE  username  = @username)
        SELECT 0,11,'give full access','No Error'
        FROM  NetworkUsers
        WHERE  username  = @username
        ELSE
        SELECT 3,0,'odbc','ODBC Authen Error'
END
```

일반 텍스트 비밀번호 인증용 파라미터를 반환하는 샘플 절차(Microsoft SQL Server용)

```
CREATE PROCEDURE [dbo].[ISEAuthUserPlainReturnsParameters]
       @username varchar(64), @password varchar(255), @result INT OUTPUT, @group varchar(255)
 OUTPUT, @acctInfo varchar(255) OUTPUT, @errorString varchar(255) OUTPUT
AS
BEGIN
        IF EXISTS( SELECT  username
        FROM  NetworkUsers
        WHERE  username  = @username
        AND  password  = @password )
        SELECT @result=0, @group=11, @acctInfo='give full access', @errorString='No Error'
        FROM  NetworkUsers
        WHERE  username  = @username
        ELSE
        SELECT @result=3, @group=0, @acctInfo='odbc',  @errorString='ODBC Authen Error'
END
```

일반 텍스트 비밀번호 가져오기용 파라미터를 반환하는 샘플 절차(Microsoft SQL Server용)

```
CREATE PROCEDURE [dbo].[ISEFetchPasswordReturnsParameters]
        @username varchar(64), @result INT OUTPUT, @group varchar(255) OUTPUT, @acctInfo
varchar(255) OUTPUT, @errorString varchar(255) OUTPUT, @password varchar(255) OUTPUT
AS
BEGIN
        IF EXISTS( SELECT  username
        FROM  NetworkUsers
        WHERE  username  = @username)
       SELECT @result=0, @group=11, @acctInfo='give full access', @errorString='No Error',
 @password=password
        FROM  NetworkUsers
        WHERE  username  = @username
        ELSE
        SELECT @result=3, @group=0, @acctInfo='odbc', @errorString='ODBC Authen Error'
END
```

조회용 파라미터를 반환하는 샘플 절차(Microsoft SQL Server용)

```
CREATE PROCEDURE [dbo].[ISEUserLookupReturnsParameters]
        @username varchar(64), @result INT OUTPUT, @group varchar(255) OUTPUT, @acctInfo
varchar(255) OUTPUT, @errorString varchar(255) OUTPUT
AS
BEGIN
        IF EXISTS( SELECT  username
        FROM  NetworkUsers
        WHERE  username  = @username)
        SELECT @result=0, @group=11, @acctInfo='give full access', @errorString='No Error'
        FROM  NetworkUsers
        WHERE  username  = @username
        ELSE
        SELECT @result=3, @group=0, @acctInfo='odbc', @errorString='ODBC Authen Error'
END
```

Microsoft SQL Server에서 그룹을 가져오는 샘플 절차

```
CREATE PROCEDURE [dbo].[ISEGroupsH]
        @username varchar(64), @result int output
AS
BEGIN
        if exists (select * from NetworkUsers where username = @username)
        begin
                set @result = 0
                select 'accountants', 'engineers', 'sales','test_group2'
        end
        else
                set @result = 1
END
```

사용자 이름이 "*"인 경우 모든 사용자의 모든 그룹을 가져오는 샘플 절차(Microsoft SQL Server용)

```
ALTER PROCEDURE [dbo].[ISEGroupsH]
                @username varchar(64), @result int output
AS
BEGIN
                if @username = '*'
                begin
                                -- if username is equal to '*' then return all existing
groups
                                set @result = 0
                                select 'accountants', 'engineers',
'sales','test_group1','test_group2','test_group3','test_group4'
```

```
                end
                else
                if exists (select * from NetworkUsers where username = @username)
                begin
                                set @result = 0
                                select 'accountants'
                end
                else
                                set @result = 1
END
```

Microsoft SQL Server에서 속성을 가져오는 샘플 절차

```
CREATE PROCEDURE [dbo].[ISEAttrsH]
        @username varchar(64), @result int output
AS
BEGIN
        if exists (select * from NetworkUsers where username = @username)
        begin
                set @result = 0
                                select phone as phone, username as username, department as
 department, floor as floor, memberOf as memberOf, isManager as isManager from NetworkUsers
 where username = @username
        end
        else
                set @result = 1
END
```

ODBC 컨피그레이션에 대한 추가적인 예

https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/211581-Configure-ODBC-on-ISE-2-3-with-Oracle-Da.html

https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine-21/200544-Configure-ISE-2-1-with-MS-SQL-using-ODBC.html

https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine-21/200644-Configure-ODBC-on-ISE-2-1-with-PostgreSQ.html

ODBC ID 소스 추가

시작하기 전에

다음 작업을 수행하려면 슈퍼 관리자 또는 시스템 관리자여야 합니다.

단계 **1** **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **External Identity Sources(**외부 **ID** 소스**)**Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 .

단계 **2** **ODBC**를 클릭합니다.

단계 **3** **Add(**추가**)**를 클릭합니다.

단계 **4** **General(**일반**)** 탭에서 ODBC ID 소스의 이름과 설명을 입력합니다.

단계 **5** **Connection(**연결**)** 탭에서 다음 세부정보를 입력합니다.

- ODBC 데이터베이스의 호스트 이름 또는 IP 주소입니다. 데이터베이스에 비표준 TCP 포트를 사용 중인 경우, 호스트 이름 또는 IP 주소:포트 형식으로 포트 번호를 지정할 수 있습니다.
- ODBC 데이터베이스의 이름

- 관리자 사용자 이름 및 비밀번호(Cisco ISE는 이러한 자격 증명을 사용하여 데이터베이스에 연결함)
- 서버 시간 초과(초)(기본값은 5초)
- 연결 시도 횟수(기본값은 1)
- 데이터베이스 유형입니다. 다음 중 하나를 선택합니다.
  - **MySQL**
  - **Oracle**
  - **PostgreSQL**
  - **Microsoft SQL Server**
  - **Sybase**

단계 **6** ODBC 데이터베이스와의 연결을 확인하고 구성된 활용 사례에 대해 저장 절차가 있는지를 확인하려면 **Test Connection(**연결 테스트**)**을 클릭합니다.

단계 **7** **Stored Procedures(**저장 절차**)** 탭에서 다음 세부정보를 입력합니다.

- **Stored Procedure Type(**저장 절차 유형**)**: 데이터베이스가 제공하는 출력 유형을 선택합니다.
  - **Returns Recordset(**기록 집합 반환**)**: 데이터베이스가 ODBC 쿼리에 대한 응답으로 기록 집합을 반환합니다.
  - **Returns Parameters(**파라미터 반환**)**: 데이터베이스가 ODBC 쿼리에 대한 응답으로 명명된 파라미터 집합을 반환합니다.
- **Plain Text Password Authentication(**일반 텍스트 비밀번호 인증**)**: 일반 텍스트 비밀번호 인증을 위해 ODBC 서버에서 실행되는 저장 절차의 이름을 입력합니다. PAP, EAP-GTC 내부 방법 및 TACACS에 사용됩니다.
- **Plain Text Password Fetching(**일반 텍스트 비밀번호 가져오기**)**: 일반 텍스트 비밀번호를 가져오기 위해 ODBC 서버에서 실행되는 저장 절차의 이름을 입력합니다. CHAP, MS-CHAPv1/v2, LEAP, EAP-MD5, EAP-MSCHAPv2 내부 방법 및 TACACS에 사용됩니다.
- **Check Username or Machine Exists(**사용자 이름 또는 머신 유무 확인**)**: 사용자/MAC 주소 조회용으로 ODBC 서버에서 실행되는 저장 절차의 이름을 입력합니다. MAB 및 PEAP, EAP-FAST, EAP-TTLS의 빠른 재연결에 사용됩니다.
- **Fetch Groups(**그룹 가져오기**)**: ODBC 데이터베이스에서 그룹을 검색하는 저장 절차의 이름을 입력합니다.
- **Fetch Attributes(**속성 가져오기**)**: ODBC 데이터베이스에서 속성 및 해당 값을 검색하는 저장 절차의 이름을 입력합니다.
- **Advanced Settings(**고급 설정**)**: 이 옵션을 클릭하면 **Fetch Attributes(**속성 가져오기**)** 저장 절차에서 다음의 사전 아래에 있는 속성을 사용자 이름 및 비밀번호와 함께 입력 매개 변수로 사용할 수 있습니다.
  - **RADIUS**
  - 디바이스

- 네트워크 액세스

참고 **Network Access(**네트워크 액세스**)** 사전의 속성은 **AuthenticationMethod**, **Device IP Address**, **EapAuthentication**, **EapTunnel**, **ISE Host Name**, **Protocol**, **UserName**, **VN**, **WasMachineAuthenticated** 만 사용할 수 있습니다.

Attribute Name in Stored Procedure(저장된 절차의 속성 이름**)** 필드에서, 저장 절차에 사용되는 속성 이름을 지정합니다.

ODBC 데이터베이스에서 다음의 출력 매개 변수를 검색하도록 저장 절차를 구성할 수 있습니다.

- ACL
- Security Group(보안 그룹)
- VLAN(이름 또는 번호)
- 웹 리디렉션 ACL
- 웹 리디렉션 포털 이름

이러한 속성을 사용하여 권한 부여 프로파일을 구성할 수 있습니다. 이러한 속성은 **Authorization Profiles(**권한 부여 프로파일**)** 창의 **Common Tasks(**일반 작업**)** 섹션에 나열됩니다(**Policy (**정책**) > Policy Elements (**정책 요소**) > Results (**결과**)**). 다음은 이러한 속성을 사용할 수 있는 몇 가지 샘플 활용 사례 시나리오입니다.

- 각 권한 부여 프로파일에 대해 VLAN을 수동으로 지정하지 않고, 지정된 입력 속성(MAC 주소, 사용자 이름, called-station-ID 또는 디바이스 위치)을 기반으로 ODBC 데이터베이스에서 반환되는 VLAN을 사용하도록 권한 부여 프로파일을 구성하는 경우.
- ODBC ID 저장소에서 차단된 호출 스테이션 ID에 대한 액세스를 차단하도록 권한 부여 프로파일을 구성하는 경우.
- MAC 주소, 사용자 이름, called-station-ID 또는 디바이스 위치를 기반으로 ODBC 데이터베이스에서 웹 리디렉션 ACL 또는 웹 리디렉션 포털 이름을 검색하도록 권한 부여 프로파일을 구성하는 경우.

권한 부여 정책을 구성하는 동안, ODBC 데이터베이스에서 검색되는 보안 그룹을 **Policy Sets(**정책 집합**)** 창에서 선택할 수 있습니다.

참고 **Advanced Settings(**고급 설정**)** 옵션을 사용하는 동안에는 추가 세부정보를 저장하기 위해 user_attributes_detail이라는 새 표가 ODBC 데이터베이스에 생성됩니다. 모든 출력 매개 변수에 대해 데이터 유형을 VARCHAR2로 설정해야합니다. 그러지 않으면 통합 및 컴파일 프로세스 중에 저장 절차가 실패할 수 있습니다. 예를 들어 SGTNAME이 VARCHAR2로 설정되고 VLANNUMBER가 NUMBER로 설정된 경우 다음 저장 절차의 컴파일이 실패할 수 있습니다.

```
select  ATTR_NAME, value from ATTRIBUTES where user_id=userid
          union
         select 'SGTNAME', SGTNAME from user_attributes_detail where USER_ID = userid and
 user_attributes_detail.DEVICELOCATIONS=ise_DEVICETYPE
          union
          select 'VLANNUMBER', VLANNUMBER from user_attributes_detail where USER_ID =
userid and user_attributes_detail.DEVICELOCATIONS=ise_DEVICETYPE;
```

- **Search for MAC Address in Format(**다음 형식으로 **MAC** 주소 검색**)**: 선택한 MAC 형식을 기준으로 수신 MAC 주소가 정규화됩니다.

단계 **8** **Attributes(**속성**)** 탭에서 필요한 속성을 추가합니다. 속성을 추가할 때는 권한 부여 정책 규칙에서 속성 이름이 표시되어야 하는 방법을 지정할 수 있습니다.

또한 ODBC 데이터베이스에서 속성을 가져올 수도 있습니다. 이러한 속성은 권한 부여 정책에서 사용할 수 있습니다.

단계 **9** **Groups(**그룹**)** 탭에서 사용자 그룹을 추가합니다. 사용자 이름 또는 MAC 주소를 지정하여 ODBC 데이터베이스에서 그룹을 가져올 수도 있습니다. 이러한 그룹은 권한 부여 정책에서 사용할 수 있습니다.

그룹과 속성의 이름을 바꿀 수 있습니다. 기본적으로 **Name in ISE(ISE** 내 이름**)** 필드에 표시되는 이름은 ODBC 데이터베이스의 이름과 같지만 이 이름은 수정할 수 있습니다. 이 이름은 권한 부여 정책에서 사용 됩니다.

단계 **10** **Submit(**제출**)**을 클릭합니다.

ODBC ID 소스를 구성하는 방법에 대한 자세한 내용은 다음 링크를 참조하십시오.

- Oracle 데이터베이스를 사용하여 Cisco ISE에서 ODBC 구성
- ODBC를 사용하여 MS SQL로 Cisco ISE 구성
- PostgreSQL을 사용하여 Cisco ISE에서 ODBC 구성
- Cisco 서버와의 통합을 위한 Cisco ISE 구성

참고 입력 속성을 구성한 경우 ODBC ID 저장소를 복제하는 동안 다음을 수행해야 합니다. 그러지 않으면 중복된 ODBC ID 저장소에서 입력 매개 변수가 손실될 수 있습니다.

1. **Advanced Settings(**고급 설정**)**를 클릭합니다.
2. 입력 매개 변수가 올바르게 설정되었는지 확인합니다.
3. **OK(**확인**)**를 클릭하여 이러한 입력 매개 변수를 중복된 ODBC ID 저장소에 저장합니다.

RADIUS 토큰 ID 소스

RADIUS 프로토콜을 지원하고 사용자 및 디바이스에 AAA(Authentication, Authorization, and Accounting) 서비스를 제공하는 서버를 RADIUS 서버라고 합니다. RADIUS ID 소스는 주체 및 자격 증명 모음이 포함되어 있는 외부 ID 소스로, 통신에 RADIUS 프로토콜을 사용합니다. 예를 들어 Safeword 토큰 서버는 여러 사용자 및 자격 증명을 일회용 비밀번호로 포함할 수 있는 ID 소스로, RADIUS 프로토콜을 사용하여 쿼리할 수 있는 인터페이스를 제공합니다.

Cisco ISE는 외부 ID 소스로 RADIUS RFC 2865 준수 서버를 지원합니다. Cisco ISE는 여러 RADIUS 토큰 서버 ID(예: RSA SecurID 서버 및 SafeWord 서버)를 지원합니다. RADIUS ID 소스는 사용자를 인증하는 데 사용되는 모든 RADIUS 토큰 서버와 연동될 수 있습니다.

참고 MAB 인증을 위해 Process Host Lookup(프로세스 호스트 조회) 옵션을 활성화해야 합니다. MAB 인증을 사용하는 디바이스는 OTP 또는 RADIUS 토큰(RADIUS 토큰 서버 인증에 필요)을 생성 할 수 없으므로 MAB 인증을 위해 외부 ID 소스로 사용되는 RADIUS 토큰 서버를 구성하지 않는 것이 좋습니다. 따라서 인증이 실패합니다. 외부 RADIUS 서버 옵션을 사용하여 MAB 요청을 처리할 수 있습니다.

RADIUS 토큰 서버에서 지원되는 인증 프로토콜

Cisco ISE는 RADIUS ID 소스에 다음 인증 프로토콜을 지원합니다.

- RADIUS PAP
- 내부 EAP-GTC(Extensible Authentication Protocol-Generic Token Card)가 있는 PEAP(Protected Extensible Authentication Protocol)
- 내부 EAP-GTC가 있는 EAP-FAST

통신에 RADIUS 토큰 서버가 사용하는 포트

RADIUS 토큰 서버는 인증 세션에 UDP 포트를 사용합니다. 이 포트는 모든 RADIUS 통신에 사용됩니다. Cisco ISE에서 RADIUS OTP(One-Time Password) 메시지를 RADIUS 지원 토큰 서버로 보내려면 Cisco ISE와 RADIUS 지원 토큰 서버 사이의 게이트웨이 디바이스가 UDP 포트를 통한 통신을 허용하는지 확인해야 합니다. 관리 포털을 통해 UDP 포트를 구성할 수 있습니다.

RADIUS 공유 암호

Cisco ISE에서 RADIUS ID 소스를 구성하면서 공유 암호를 제공해야 합니다. 이 공유 암호는 RADIUS 토큰 서버에 구성된 공유 암호와 동일해야 합니다.

RADIUS 토큰 서버의 페일오버

Cisco ISE에서는 여러 RADIUS ID 소스를 구성할 수 있습니다. 각 RADIUS ID 소스마다 기본 및 보조 RADIUS 서버가 있을 수 있습니다. Cisco ISE가 기본 서버에 연결할 수 없는 경우에는 보조 서버를 사용합니다.

RADIUS 토큰 서버에서 구성 가능한 비밀번호 프롬프트

RADIUS ID 소스에서는 비밀번호 프롬프트를 구성할 수 있습니다. 관리 포털을 통해 비밀번호 프롬프트를 구성할 수 있습니다.

RADIUS 토큰 서버 사용자 인증

Cisco ISE는 사용자 자격 증명(사용자 이름 및 비밀번호)을 가져와 RADIUS 토큰 서버에 전달합니다. Cisco ISE는 또한 RADIUS 토큰 서버 인증 처리 결과를 사용자에게 릴레이합니다.

RADIUS 토큰 서버의 사용자 속성 캐시

RADIUS 토큰 서버는 기본적으로 사용자 조회를 지원하지 않습니다. 그러나 사용자 조회는 다음 Cisco ISE 기능에 필수적인 기능입니다.

- PEAP 세션 재개: 이 기능은 EAP 세션을 설정하는 중에 성공적인 인증이 이루어지면 PEAP 세션을 재개하도록 합니다.
- EAP/FAST 빠른 재연결: 이 기능은 EAP 세션을 설정하는 중에 성공적인 인증이 이루어지면 빠른 재연결을 허용합니다.
- TACACS + 권한 부여: TACACS + 인증에 성공한 후 발생합니다.

Cisco ISE는 성공적인 인증 결과를 캐시하여 이러한 기능에 대한 사용자 조회 요청을 처리합니다. 각각의 성공적인 인증에서 인증된 사용자의 이름 및 검색된 속성이 캐시됩니다. 실패한 인증은 캐시에 기록되지 않습니다.

런타임에 메모리에서 캐시를 사용할 수 있으며 캐시는 분산형 구축의 Cisco ISE 노드 간에 복제되지 않습니다. 관리 포털을 통해 TTL(Time to Live) 제한을 구성할 수 있습니다. ISE 2.6부터는 ID 캐싱 옵션을 활성화하고 에이징 타임을 분 단위로 설정할 수 있습니다. 이 옵션은 기본적으로 비활성화되어 있으며, 활성화된 경우 지정된 시간 동안 메모리에서 캐시를 사용할 수 있습니다.

ID 시퀀스의 RADIUS ID 소스

ID 소스 시퀀스에서 인증 시퀀스의 RADIUS ID 소스를 추가할 수 있습니다. 그러나 인증 없이 RADIUS ID 소스를 쿼리할 수 없으므로 속성 검색 시퀀스의 RADIUS ID 소스를 추가할 수 없습니다. Cisco ISE는 RADIUS 서버를 인증하는 동안 서로 다른 오류를 구분할 수 없습니다. RADIUS 서버는 모든 오류에 대해 Access-Reject 메시지를 반환합니다. 예를 들어 RADIUS 서버에 사용자가 없으면 RADIUS 서버는 사용자 알 수 없음 상태를 반환하는 대신 RADIUS 서버는 Access-Reject 메시지를 반환합니다.

RADIUS 서버가 모든 오류에 대해 같은 메시지를 반환함

RADIUS 서버에 사용자가 없으면 RADIUS 서버는 Access-Reject 메시지를 반환합니다. Cisco ISE는 관리 포털을 통해 이 메시지를 인증 실패 또는 사용자를 찾을 수 없음 메시지로 구성할 수 있는 옵션을 제공합니다. 그러나 이 옵션은 사용자를 확인할 수 없는 사례뿐 아니라 모든 오류 사례에 대해 사용자를 찾을 수 없음 메시지를 반환합니다.

다음 표에는 RADIUS ID 서버에서 발생할 수 있는 다양한 오류 사례가 나열되어 있습니다.

표 37: 오류 처리

오류 사례	오류 이유
인증 실패	• 사용자를 확인할 수 없습니다. • 사용자가 잘못된 암호로 로그인을 시도했습니다. • 사용자 로그인 시간이 만료 되었습니다.
처리 실패	• RADIUS 서버가 Cisco ISE에서 잘못 구성되어 있습니다. • RADIUS 서버를 사용할 수 없습니다. • RADIUS 패킷의 형식이 잘못된 것으로 탐지되었습니다. • RADIUS 서버에서 패킷을 보내거나 받는 동안 문제가 발생했습니다. • 시간이 초과되었습니다.
알 수 없는 사용자	인증이 실패했으며 Fail on Reject(거부 시 실패) 옵션이 false로 설정되어 있습니다.

SafeWord 서버의 특수 사용자 이름 형식 지원

SafeWord 토큰 서버는 다음 사용자 이름 형식을 사용하는 인증을 지원합니다.

사용자 이름 - 사용자 이름, OTP

Cisco ISE는 인증 요청을 받는 즉시 사용자 이름을 구문 분석하여 다음 사용자 이름으로 변환합니다.

사용자 이름 - 사용자 이름

SafeWord 토큰 서버는 이 두 가지 형식을 모두 지원합니다. Cisco ISE에서는 다양한 토큰 서버를 사용합니다. SafeWord 서버를 구성할 때는 Cisco ISE의 관리 포털에서 SafeWord Server(SafeWord 서버) 확인란을 선택하여 사용자 이름을 구문 분석하고 지정된 형식으로 변환해야 합니다. 요청이 RADIUS 토큰 서버로 전송되기 전에 RADIUS 토큰 서버 ID 소스에서 이 변환이 수행됩니다.

RADIUS 토큰 서버의 인증 요청 및 응답

Cisco ISE가 인증 요청을 RADIUS 지원 토큰 서버로 전달하는 경우 RADIUS 인증 요청에는 다음과 같은 속성이 포함됩니다.

- User-Name(RADIUS 속성 1)
- User-Password(RADIUS 속성 2)

- NAS-IP-Address(RADIUS 속성 4)

Cisco ISE가 수신을 기대하는 응답은 다음 중 하나입니다.

- Access-Accept: 속성이 필요하지 않습니다. 그러나 응답에는 RADIUS 토큰 서버 컨피그레이션에 따라 다양한 속성을 포함할 수 있습니다.
- Access-Reject: 속성이 필요하지 않습니다.
- Access-Challenge: RADIUS RFC마다 필요한 속성은 다음과 같습니다.
  - State(RADIUS 속성 24)
  - Reply-Message(RADIUS 속성 18)
  - 다음 속성 중 하나 이상: Vendor-Specific, Idle-Timeout(RADIUS 속성 28), Session-Timeout(RADIUS 속성 27), Proxy-State(RADIUS 속성 33)

    Access-Challenge에서 다른 속성은 허용되지 않습니다.

RADIUS 토큰 ID 소스 설정

다음 표에서는 외부 RADIUS ID 소스를 구성하고 해당 소스에 연결하는 데 사용할 수 있는 RADIUS 토큰 ID 소스 창의 필드에 대해 설명합니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **External Identity Sources(**외부 **ID** 소스**)** > **RADIUS Token(RADIUS** 토큰**)**입니다.

표 ***38: RADIUS*** 토큰 ***ID*** 소스 설정

필드 이름	사용 지침
Name(이름**)**	RADIUS 토큰 서버의 이름을 입력합니다. 최대 64자까지 입력할 수 있습니다.
Description(설명**)**	RADIUS 토큰 서버에 대한 설명을 입력합니다. 최대 문자 수는 1,024자입니다.
SafeWord Server(SafeWord 서버**)**	RADIUS ID 소스가 SafeWord 서버인 경우 이 확인란을 선택합니다.
Enable Secondary Server(보조 서버 활성화**)**	기본 서버에 오류가 발생하는 경우 백업으로 사용할 Cisco ISE용 보조 RADIUS 토큰 서버를 활성화하려면 이 확인란을 선택합니다. 이 확인란을 선택하는 경우 보조 RADIUS 토큰 서버를 구성해야 합니다.
Always Access Primary Server First(항상 기본 서버에 먼저 액세스**)**	Cisco ISE가 항상 기본 서버에 먼저 액세스하도록 하려면 이 옵션을 클릭합니다.

필드 이름	사용 지침
Fallback to Primary Server after(다음 시간 이후 기본 서버로 대체**)**	기본 서버에 연결할 수 없는 경우 Cisco ISE가 보조 RADIUS 토큰 서버를 사용하여 인증할 수 있는 시간(분)을 지정하려면 이 옵션을 클릭합니다. 이 시간이 경과하면 Cisco ISE는 기본 서버에 대한 인증을 재시도합니다.
기본 서버	
Host IP(호스트 **IP)**	기본 RADIUS 토큰 서버의 IP 주소를 입력합니다. 이 필드에는 문자열로 표시되는 유효한 IP 주소를 입력할 수 있습니다. 이 필드에 입력할 수 있는 문자는 숫자와 점(.)입니다.
Shared Secret(공유 암호**)**	이 연결에 대해 기본 RADIUS 토큰 서버에 구성된 공유 암호를 입력합니다.
Authentication Port(인증 포트**)**	기본 RADIUS 토큰 서버가 수신 대기 중인 포트 번호를 입력합니다.
Server Timeout(서버 시간 초과**)**	기본 RADIUS 토큰 서버가 다운되었다고 결정할 때까지 Cisco ISE가 기본 서버로부터의 응답을 대기할 시간을 초 단위로 지정합니다.
Connection Attempts(연결 시도 횟수**)**	Cisco ISE가 보조 서버(정의된 경우)로 이동하거나 보조 서버가 정의되어 있지 않은 경우 요청을 삭제하기 전에 기본 서버에 다시 연결을 시도해야 하는 횟수를 지정합니다.
보조 서버	
Host IP(호스트 **IP)**	보조 RADIUS 토큰 서버의 IP 주소를 입력합니다. 이 필드에는 문자열로 표시되는 유효한 IP 주소를 입력할 수 있습니다. 이 필드에 입력할 수 있는 문자는 숫자와 점(.)입니다.
Shared Secret(공유 암호**)**	이 연결에 대해 보조 RADIUS 토큰 서버에 구성된 공유 암호를 입력합니다.
Authentication Port(인증 포트**)**	보조 RADIUS 토큰 서버가 수신 대기 중인 포트 번호를 입력합니다. 유효한 값은 1~65,535입니다. 기본값은 1,812입니다.
Server Timeout(서버 시간 초과**)**	보조 RADIUS 토큰 서버가 다운되었다고 결정할 때까지 Cisco ISE가 보조 서버로부터의 응답을 대기할 시간을 초 단위로 지정합니다.
Connection Attempts(연결 시도 횟수**)**	Cisco ISE가 요청을 삭제하기 전에 보조 서버에 다시 연결을 시도해야 하는 횟수를 지정합니다.

관련 항목

RADIUS 토큰 ID 소스, 163 페이지
RADIUS 토큰 서버 추가, 169 페이지

RADIUS 토큰 서버 추가

시작하기 전에

다음 작업을 수행하려면 슈퍼 관리자 또는 시스템 관리자여야 합니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** **External Identity Sources(**외부 **ID** 소스**)** > **RADIUS Token(RADIUS** 토큰**)** > **Add(**추가**)**를 선택합니다.

단계 **2** **General(**일반**)** 및 **Connection(**연결**)** 탭에 값을 입력합니다.

단계 **3** **Authentication(**인증**)** 탭을 클릭합니다.

이 탭에서는 RADIUS 토큰 서버의 Access-Reject 메시지에 대한 응답을 제어할 수 있습니다. 이 응답은 자격 증명이 잘못되었거나 사용자를 알 수 없다는 의미일 수 있습니다. Cisco ISE는 인증 실패 또는 사용자를 찾을 수 없음 응답 중 하나를 수락합니다. 또한 이 탭에서는 ID 캐싱을 활성화하고 캐시의 에이징 시간을 설정할 수도 있습니다. 그리고 비밀번호 요청 메시지도 구성할 수 있습니다.

a) RADIUS 토큰 서버의 Access-Reject 응답을 인증 실패로 처리하려는 경우 **Treat Rejects as 'authentication failed'(**거부를 '인증 실패'로 처리**)** 라디오 버튼을 클릭합니다.

b) RADIUS 토큰 서버의 Access-Reject 응답을 알 수 없는 사용자 오류로 처리하려는 경우 **Treat Rejects as 'user not found'(**거부를 '사용자를 찾을 수 없음'으로 처리**)** 라디오 버튼을 클릭합니다.

단계 **4** Cisco ISE가 RADIUS 토큰 서버를 사용한 첫 번째 인증에 성공한 후 캐시에 암호를 저장하고 구성된 기간 내에 발생하는 경우 후속 인증에 대해 캐시된 사용자 자격 증명을 사용하도록 하려면 **Enable Passcode Caching(**암호 캐싱 활성화**)** 확인란을 선택합니다.

Aging Time(에이징 시간**)** 필드의 캐시에 암호가 저장되어야 하는 시간을 초 단위로 입력합니다. 이 기간 동안에는 사용자가 동일한 암호를 사용하여 인증을 2회 이상 수행할 수 있습니다. 기본값은 30초입니다. 유효 범위는 1~300초입니다.

참고 Cisco ISE는 첫 번째 인증 실패 후 캐시를 지웁니다. 사용자는 새 유효 암호를 입력해야 합니다.

참고 이 옵션은 예를 들어 -FAST-GTC 같은 암호의 암호화를 지원하는 프로토콜을 사용할 때만 활성화하는 것이 좋습니다. RADIUS 토큰 서버에서 지원되는 인증 프로토콜에 대한 자세한 내용은 다음을 참조하십시오. RADIUS 토큰 서버에서 지원되는 인증 프로토콜, 164 페이지

단계 **5** 서버에 대해 인증을 수행하지 않는 요청을 처리하게 하려면 **Enable Identity Caching(ID** 캐싱 활성화**)** 확인란을 선택합니다.

ID 캐싱 옵션을 활성화하고 에이징 타임을 분 단위로 설정할 수 있습니다. 기본값은 120분입니다. 유효 범위는 1분~1440분입니다. 마지막으로 성공한 인증에서 얻은 결과와 속성은 지정된 기간 동안 캐시에 보관됩니다.

이 옵션은 기본적으로 비활성화되어 있습니다.

단계 **6** **Authorization(**권한 부여**)** 탭을 클릭합니다.

이 탭에서는 Cisco ISE로 Access-Accept 응답을 보내는 중에 RADIUS 토큰 서버에서 반환하는 속성에 대해 표시할 이름을 구성할 수 있습니다. 권한 부여 정책 조건에서 이 속성을 사용할 수 있습니다. 기본값은 CiscoSecure-Group-Id입니다.

참고 외부 ID 소스에서 Access-Accept의 속성을 보내려면 Ext ID 소스가 <ciscoavpair>를 속성 이름과 값으로 전송해야 합니다. 이때 ACS:<attrname>=<attrvalue> 형식을 사용해야 하며, 여기서 <attrname>은 **Authorization(**권한 부여**)** 탭에서 구성됩니다.

단계 **7** **Submit(**제출**)**을 클릭합니다.

RADIUS 토큰 서버 삭제

시작하기 전에

- 다음 작업을 수행하려면 슈퍼 관리자 또는 시스템 관리자여야 합니다.
- ID 소스 시퀀스의 일부분인 RADIUS 토큰 서버를 선택하지 않았는지 확인합니다. ID 소스 시퀀스의 일부분인 RADIUS 토큰 서버를 삭제하도록 선택하면 삭제 작업이 실패합니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **External Identity Sources(**외부 **ID** 소스**)** > **RADIUS Token(RADIUS** 토큰**)**을 선택합니다.

단계 **2** 삭제할 하나 이상의 RADIUS 토큰 서버 옆에 있는 확인란을 선택하고 **Delete(**삭제**)**를 클릭합니다.

단계 **3** **OK(**확인**)**를 클릭하여 선택한 하나 이상의 RADIUS 토큰 서버를 삭제합니다.

여러 RADIUS 토큰 서버를 삭제하도록 선택했는데 그 중 하나가 ID 소스 시퀀스에서 사용되는 경우에는 삭제 작업이 실패하며 모든 RADIUS 토큰 서버는 삭제되지 않습니다.

RSA ID 소스

Cisco ISE는 외부 데이터베이스로 RSA SecurID 서버를 지원합니다. RSA SecurID 2단계 인증은 사용자 PIN과 개별적으로 등록된 RSA SecurID 토큰으로 이루어집니다. 이 토큰은 시간 코드 알고리즘을 기반으로 하는 일회용 토큰 코드를 생성합니다. 고정 간격(일반적으로 30초 또는 60초마다)으로 다른 토큰 코드가 생성됩니다. RSA SecurID 서버는 이 동적 인증 코드를 검증합니다. 각 RSA SecurID 토큰은 고유하며 과거의 토큰을 기반으로 미래의 토큰 값을 예측할 수 없습니다. 따라서 PIN과 함께 올바른 토큰 코드를 제공하면 개인이 유효한 사용자임을 나타내는 확실성 수준이 높아집니다. 그러므로 RSA SecurID 서버는 기존의 재사용 가능한 비밀번호보다 안정적인 인증 메커니즘을 제공합니다.

Cisco ISE는 다음과 같은 RSA ID 소스를 지원합니다.

- RSA ACE/Server 6.x Series

- RSA Authentication Manager 7.x 및 8.0 Series

다음 방법 중 하나를 사용하여 RSA SecurID 인증 기술과 통합할 수 있습니다.

- RSA SecurID 에이전트 사용: RSA 기본 프로토콜을 통해 사용자 이름 및 암호를 사용하여 사용자가 인증됩니다.
- RADIUS 프로토콜 사용: RADIUS 프로토콜을 통해 사용자 이름 및 암호를 사용하여 사용자가 인증됩니다.

Cisco ISE의 RSA SecurID 토큰 서버는 RSA SEcurID 에이전트를 사용하여 RSA SecurID 인증 기술에 연결됩니다.

Cisco ISE는 하나의 RSA 영역만 지원합니다.

Cisco ISE와 RSA SecurID 서버 통합

Cisco ISE를 RSA SecurID 서버에 연결하는 데에는 두 가지 관리 역할이 관여합니다.

- RSA 서버 관리자: RSA 시스템 및 통합을 구성하고 유지 관리합니다.
- Cisco ISE 관리자: RSA SecurID 서버에 연결되도록 Cisco ISE를 구성하고 컨피그레이션을 유지 관리합니다.

이 섹션에서는 Cisco ISE를 RSA SecurID 서버에 외부 ID 소스로 연결하는 것과 관련된 프로세스에 설명합니다. RSA 서버에 대한 자세한 내용은 RSA 설명서를 참고해 주십시오.

Cisco ISE의 RSA 컨피그레이션

RSA 관리 시스템에서는 RSA 시스템 관리자가 사용자에게 제공하는 sdconf.rec 파일을 생성합니다. 이 파일을 사용하면 영역 내 RSA SEcurID 에이전트로 Cisco ISE 서버를 추가할 수 있습니다. 이렇게 하려면 Cisco ISE에서 이 파일을 찾아서 추가해야 합니다. 기본 Cisco ISE 서버는 복제 프로세스를 통해 모든 보조 서버에 이 파일을 배포합니다.

RSA SecurID 서버에 대한 RSA 에이전트 인증

모든 Cisco ISE 서버에 sdconf.rec 파일을 설치하고 나면 RSA 에이전트 모듈이 시작되며 RSA에서 생성한 자격 증명을 사용하는 인증이 각 Cisco ISE 서버에서 진행됩니다. 구축 내 각 Cisco ISE 서버의 에이전트가 정상적으로 인증되면 RSA 서버와 에이전트 모듈은 securid 파일을 함께 다운로드합니다. 이 파일은 Cisco ISE 파일 시스템에서 RSA 에이전트가 정의한 잘 알려진 위치에 있습니다.

분산형 Cisco ISE 환경의 RSA ID 소스

분산형 Cisco ISE 환경에서 RSA ID 소스를 관리할 때는 다음 작업을 수행합니다.

- 기본 서버에서 보조 서버로 sdconf.rec 및 sdopts.rec 파일 배포
- securid 및 sdstatus.12 파일 삭제

Cisco ISE 구축에서 RSA 서버 업데이트

Cisco ISE에서 sdconf.rec 파일을 추가하고 나면 RSA SecurID 관리자가 RSA 서버를 해제하거나 새 RSA 보조 서버를 추가할 때 sdconf.rec 파일을 업데이트할 수 있습니다. 이 경우 RSA SecurID 관리자는 업데이트된 파일을 제공합니다. 그러면 업데이트된 파일을 사용하여 Cisco ISE를 재구성할 수 있습니다. Cisco ISE의 복제 프로세스에서는 업데이트된 파일을 구축의 보조 Cisco ISE 서버로 배포합니다. Cisco ISE는 먼저 파일 시스템의 파일을 업데이트한 다음 RSA 에이전트 모듈과의 조정을 통해 다시 시작 프로세스의 단계를 적절하게 지정합니다. sdconf.rec 파일이 업데이트되면 sdstatus.12 및 securid 파일이 재설정(삭제)됩니다.

자동 RSA 라우팅 재정의

영역 내에 RSA 서버가 여러 개 있을 수 있습니다. sdopts.rec 파일은 로드 밸런서 역할을 수행합니다. Cisco ISE 서버 및 RSA SecurID 서버는 에이전트 모듈을 통해 작동합니다. Cisco ISE에 있는 에이전트 모듈은 영역 내 RSA 서버를 가장 효율적으로 사용하기 위해 비용 기반 라우팅 표을 유지 관리합니다. 그러나 관리 포털을 통해 sdopts.rec라는 텍스트 파일을 사용하면 영역의 각 Cisco ISE 서버에 대해 수동 컨피그레이션을 수행하여 이 라우팅을 재정의하도록 선택할 수 있습니다. 이 파일을 생성하는 방법에 대한 자세한 내용은 RSA 설명서를 참고해 주십시오.

RSA 노드 암호 재설정

securid 파일은 암호 노드 키 파일입니다. RSA는 처음 설정될 때 암호를 사용하여 에이전트를 검증합니다. Cisco ISE에 상주하는 RSA 에이전트는 처음으로 RSA 서버에 정상 인증되면 클라이언트 머신에 securid 파일을 생성한 다음 머신 간에 교환되는 데이터가 유효한지를 확인하는 데 사용합니다. RSA 서버에서 키를 재설정한 후와 같이 경우에 따라 구축의 특정 Cisco ISE 서버 또는 서버 그룹에서 securid 파일을 삭제해야 할 수 있습니다. Cisco ISE 관리 포털을 사용하여 해당 영역에 대해 Cisco ISE 서버에서 이 파일을 삭제할 수 있습니다. Cisco ISE의 RSA 에이전트는 다음 번에 정상 인증되면 새 securid 파일을 생성합니다.

참고 Cisco ISE의 최신 릴리스로 업그레이드한 후 인증이 실패하면 RSA 암호를 재설정해 주십시오.

RSA 자동 가용성 재설정

sdstatus.12 파일은 영역 내 RSA 서버의 가용성에 대한 정보를 제공합니다. 예를 들어 활성 상태인 서버와 다운된 서버에 대한 정보를 제공합니다. 에이전트 모듈은 영역 내 RSA 서버에서 작동하여 이 가용성 상태를 유지 관리합니다. 이 정보는 sdstatus.12 파일에서 연속으로 나열되며 Cisco ISE 파일 시스템의 잘 알려진 위치에서 제공됩니다. 이 파일이 오래되어 최신 상태가 이 파일에 반영되지 않는 경우도 있습니다. 이러한 경우에는 최신 상태가 다시 생성되도록 이 파일을 제거해야 합니다. 관리 포털을 사용하여 특정 영역에 대해 특정 Cisco ISE 서버에서 파일을 삭제할 수 있습니다. Cisco ISE는 RSA 에이전트와의 조정을 통해 올바른 다시 시작 단계를 지정합니다.

securid 파일이 재설정되거나 sdconf.rec 또는 sdopts.rec 파일이 업데이트될 때마다 sdstatus.12가 삭제됩니다.

RSA SecurID ID 소스 설정

다음 표에서는 RSA SecurID ID 소스를 생성하고 해당 소스에 연결하는 데 사용할 수 있는 RSA SecurID ID 소스 페이지의 필드에 대해 설명합니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **External Identity Sources(**외부 **ID** 소스**)** > **RSA SecurID**입니다.

RSA 프롬프트 설정

다음 표에서는 **RSA Prompts(RSA** 프롬프트**)** 탭의 필드에 대해 설명합니다.

표 ***39: RSA*** 프롬프트 설정

필드 이름	사용 지침
Enter Passcode Prompt(암호 프롬프트 입력**)**	암호를 가져오기 위한 텍스트 문자열을 입력합니다.
Enter Next Token Code(다음 토큰 코드 입력**)**	다음 토큰을 요청하기 위한 텍스트 문자열을 입력합니다.
Choose PIN Type(PIN 유형 선택**)**	PIN 유형을 요청하기 위한 텍스트 문자열을 입력합니다.
Accept System PIN(시스템 **PIN** 수락**)**	시스템에서 생성된 핀 번호를 수락하기 위한 텍스트 문자열을 입력합니다.
Enter Alphanumeric PIN(영숫자 **PIN** 입력**)**	영숫자 PIN을 요청하기 위한 텍스트 문자열을 입력합니다.
Enter Numeric PIN(숫자 **PIN** 입력**)**	숫자 PIN을 요청하기 위한 텍스트 문자열을 입력합니다.
Re-enter PIN(PIN 다시 입력**)**	사용자에게 PIN을 다시 입력하도록 요청하기 위한 텍스트 문자열을 입력합니다.

RSA 메시지 설정

다음 표에서는 **RSA Messages(RSA** 메시지**)** 탭의 필드에 대해 설명합니다.

표 ***40: RSA*** 메시지 설정

필드 이름	사용 지침
Display System PIN Message(시스템 **PIN** 메시지 표시**)**	시스템 PIN 메시지에 레이블을 지정하기 위한 텍스트 문자열을 입력합니다.
Display System PIN Reminder(시스템 **PIN** 알림 표시**)**	사용자에게 새 PIN을 저장하도록 알리기 위한 텍스트 문자열을 입력합니다.

필드 이름	사용 지침
Must Enter Numeric Error(숫자를 입력해야 함 오류**)**	사용자에게 PIN에 숫자만 입력해야 하도록 지시하기 위한 메시지를 입력합니다.
Must Enter Alpha Error(영숫자를 입력해야 함 오류**)**	사용자에게 PIN에 영숫자 문자만 입력해야 하도록 지시하기 위한 메시지를 입력합니다.
PIN Accepted Message(PIN 수락됨 메시지**)**	사용자의 PIN이 시스템에서 수락되면 표시되는 메시지를 입력합니다.
PIN Rejected Message(PIN 거부됨 메시지**)**	시스템에서 사용자의 PIN을 거부하면 표시되는 메시지를 입력합니다.
User Pins Differ Error(사용자 **PIN**이 다름 오류**)**	사용자가 잘못된 PIN을 입력하면 표시되는 메시지를 입력합니다.
System PIN Accepted Message(시스템이 **PIN**을 수락함 메시지**)**	시스템에서 PIN을 수락하면 사용자에게 표시되는 메시지를 입력합니다.
Bad Password Length Error(잘못된 비밀번호 길이 오류**)**	사용자가 지정한 PIN이 PIN 길이 정책에 지정된 범위를 벗어나면 표시되는 메시지를 입력합니다.

관련 항목

RSA ID 소스, 170 페이지
Cisco ISE와 RSA SecurID 서버 통합, 171 페이지
RSA ID 소스 추가, 174 페이지

RSA ID 소스 추가

RSA ID 소스를 생성하려면 RSA 구성 파일(sdconf.rec)을 가져와야 합니다. sdconf.rec 파일은 RSA 관리자에게 받아야 합니다. 이 작업을 수행하려면 슈퍼 관리자 또는 시스템 관리자여야 합니다.

RSA ID 소스를 추가할 때는 다음 작업을 수행합니다.

RSA 구성 파일 가져오기

Cisco ISE에서 RSA ID 소스를 추가하려면 RSA 구성 파일을 가져와야 합니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **External Identity Sources(**외부 **ID** 소스**)** > **RSA SecurID** > **Add(**추가**)**를 선택합니다.

단계 **2** **Browse(**찾아보기**)**를 클릭하여 클라이언트 브라우저를 실행 중인 시스템에서 신규 또는 업데이트된 sdconf.rec 파일을 선택합니다.

RSA ID 소스를 처음 생성할 때는 Import new sdconf.rec(새 sdconf.rec 파일 가져오기) 필드가 필수 필드로 지정됩니다. 그 이후에는 필요한 경우에 한해 기존 sdconf.rec 파일을 업데이트된 파일로 교체할 수 있습니다.

단계 **3** 서버 시간 초과 값을 초 단위로 입력합니다. Cisco ISE는 지정된 시간 동안 RSA 서버의 응답을 대기한 후 시간 초과됩니다. 이 값은 1~199 사이의 정수일 수 있습니다. 기본값은 30초입니다.

단계 **4** PIN 변경 시 재인증을 강제로 수행하려면 **Reauthenticate on Change PIN(PIN** 변경 시 재인증**)** 확인란을 선택합니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

Cisco ISE에서는 다음 시나리오도 지원합니다.

- Cisco ISE 서버의 옵션 파일을 구성하고 SecurID 및 sdstatus.12 파일 재설정
- RSA ID 소스에 대한 인증 제어 옵션 구성

Cisco ISE 서버의 옵션 파일을 구성하고 SecurID 및 sdstatus.12 파일 재설정

단계 **1** Cisco ISE 서버에 로그인합니다.

단계 **2** **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **External Identity Sources(**외부 **ID** 소브**)** > **RSA SecurID** > **Add(**추가**)**를 선택합니다.

단계 **3** **RSA Instance Files(RSA** 인스턴스 파일**)** 탭을 클릭합니다.

이 페이지에는 구축 내 모든 Cisco ISE 서버의 sdopts.rec 파일이 나열됩니다.

사용자가 RSA SecurID 토큰 서버에 대해 인증되면 노드 암호 상태가 *Created(*생성됨*)*로 표시됩니다. 노드 암호 상태는 Create(생성됨) 또는 Not Created(생성되지 않음) 중 하나일 수 있습니다. 지워진 노드의 노드 암호 상태는 *Not Created(*생성되지 않음*)*로 표시됩니다.

단계 **4** 특정 Cisco ISE 서버의 sdopts.rec 파일 옆에 있는 라디오 버튼을 클릭하고 **Update Options File(**옵션 파일 업데이트**)**을 클릭합니다.

기존 파일이 현재 파일 영역에 표시됩니다.

단계 **5** 다음 중 하나를 선택합니다.

- Use the Automatic Load Balancing status maintained by the RSA agent(RSA 에이전트가 유지 관리하는 자동 로드 밸런싱 상태 사용) - RSA 에이전트가 로드 밸런싱을 자동으로 관리하도록 하려면 이 옵션을 선택합니다.
- Override the Automatic Load Balancing status with the sdopts.rec file selected below(아래에서 선택한 sdopts.rec 파일을 사용하여 자동 로드 밸런싱 상태 재정의) - 특정 요구에 따라 로드 밸런싱을 수동으로 구성하려면 이 옵션을 선택합니다. 이 옵션을 선택하는 경우 **Browse(**찾아보기**)**를 클릭하여 클라이언트 브라우저를 실행 중인 시스템에서 새 sdopts.rec 파일을 선택해야 합니다.

단계 **6** **OK(**확인**)**를 클릭합니다.

단계 **7** Cisco ISE 서버에 해당하는 행을 클릭하여 해당 서버에 대한 securid 및 sdstatus.12 파일을 재설정합니다.

a) 드롭다운 화살표를 클릭하고 securid 파일 재설정 및 sdstatus.12 파일 재설정 열에서 **Remove on Submit(**제출 시 제거**)**을 선택합니다.

참고 Reset sdstatus.12 File(sdstatus.12 파일 재설정) 필드는 보기에서 숨겨져 있습니다. 이 필드를 표시하려면 맨 안쪽 프레임의 세로 및 가로 스크롤 막대를 사용하여 아래쪽과 오른쪽으로 차례로 스크롤합니다.

b) 변경사항을 저장하려면 이 행에서 **Save(**저장**)**를 클릭합니다.

단계 **8** **Save(**저장**)**를 클릭합니다.

RSA ID 소스에 대한 인증 제어 옵션 구성

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **External Identity Sources(**외부 **ID** 소스**)** > **RSA SecurID** > **Add(**추가**)**를 선택합니다.

단계 **2** **Authentication Control(**인증 제어**)** 탭을 클릭합니다.

단계 **3** 다음 중 하나를 선택합니다.

- Treat Rejects as "authentication failed"(거부를 "인증 실패"로 처리) - 거부된 요청을 실패한 인증으로 처리하려는 경우 이 옵션을 선택합니다.
- Treat Rejects as "user not found"(거부를 "사용자를 찾을 수 없음"으로 처리) - 거부된 요청을 사용자를 찾을 수 없음 오류로 처리하려는 경우 이 옵션을 선택합니다.

단계 **4** Cisco ISE가 첫 번째 인증에 성공한 후 캐시에 암호를 저장하고 구성된 기간 내에 발생하는 경우 후속 인증에 대해 캐싱된 사용자 자격 증명을 사용하도록 하려면 **Enable Passcode Caching(**암호 캐싱 활성화**)** 확인란을 선택합니다.

Aging Time(에이징 시간**)** 필드의 캐시에 암호가 저장되어야 하는 시간을 초 단위로 입력합니다. 이 기간 동안에는 사용자가 동일한 암호를 사용하여 인증을 2회 이상 수행할 수 있습니다. 기본값은 30초입니다. 유효 범위는 1~300초입니다.

참고 Cisco ISE는 첫 번째 인증 실패 후 캐시를 지웁니다. 사용자는 새 유효 암호를 입력해야 합니다.

참고 이 옵션은 예를 들어 -FAST-GTC 같은 암호의 암호화를 지원하는 프로토콜을 사용할 때만 활성화하는 것이 좋습니다.

단계 **5** 서버에 대해 인증을 수행하지 않는 요청을 처리하게 하려면 **Enable Identity Caching(ID** 캐싱 활성화**)** 확인란을 선택합니다.

ID 캐싱 옵션을 활성화하고 에이징 타임을 분 단위로 설정할 수 있습니다. 기본값은 120분입니다. 유효 범위는 1분~1440분입니다. 마지막으로 성공한 인증에서 얻은 결과와 속성은 지정된 기간 동안 캐시에 보관됩니다.

이 옵션은 기본적으로 비활성화되어 있습니다.

단계 **6** 컨피그레이션을 저장하려면 **Save(**저장**)**를 클릭합니다.

RSA 프롬프트 구성

Cisco ISE에서는 RSA SecurID 서버로 전송되는 요청을 처리하는 동안 사용자에게 제공되는 RSA 프롬프트를 구성할 수 있습니다.

시작하기 전에

다음 작업을 수행하려면 슈퍼 관리자 또는 시스템 관리자여야 합니다.

단계 **1** **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **External Identity Sources(**외부 **ID** 소스**)** > **RSA SecurID**Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 .

단계 **2** **Prompts(**프롬프트**)**를 클릭합니다.

단계 **3** RSA SecurID ID 소스 설정의 설명에 따라 값을 입력합니다.

단계 **4** **Submit(**제출**)**을 클릭합니다.

RSA 메시지 구성

Cisco ISE에서는 RSA SecurID 서버로 전송되는 요청을 처리하는 동안 사용자에게 제공되는 메시지를 구성할 수 있습니다.

시작하기 전에

다음 작업을 수행하려면 슈퍼 관리자 또는 시스템 관리자여야 합니다.

단계 **1** **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **External Identity Sources(**외부 **ID** 소스**)** > **RSA SecurID**Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 .

단계 **2** **Prompts(**프롬프트**)**를 클릭합니다.

단계 **3** **Messages(**메시지**)** 탭을 클릭합니다.

단계 **4** RSA SecurID ID 소스 설정의 설명에 따라 값을 입력합니다.

단계 **5** **Submit(**제출**)**을 클릭합니다.

외부 ID 소스로서의 SAMLv2 ID 제공자

SAML(Security Assertion Markup Language)은 관리자가 정의된 애플리케이션 중 하나에 로그인한 후에 해당 애플리케이션에 원활히 액세스하도록 해주는 XML 기반의 개방형 표준 데이터 형식입니다. SAML은 신뢰할 수 있는 비즈니스 파트너 간의 보안 관련 정보 교환에 대해 설명합니다. SAML은 IdP(Identity Provider)와 통신 사업자(이 경우 ISE) 간에 보안 인증 정보 교환을 가능하게 합니다.

SAML SSO(Single Sign On)는 메타데이터 및 인증서를 프로비저닝 프로세스의 일부로 IdP와 서비스 제공자 간에 교환하여 CoT(Circle of Trust)를 설정합니다. 서비스 제공자는 IdP의 사용자 정보를 신뢰하여 다양한 서비스 또는 애플리케이션에 대한 액세스를 제공합니다.

SAML SSO를 사용하면 다음과 같이 다양한 이점을 얻을 수 있습니다.

- 서로 다른 사용자 이름 및 비밀번호 조합을 입력하지 않아도 되므로 비밀번호를 사용하는 데 따르는 번거로움이 줄어듭니다.
- 동일한 ID에 대한 자격 증명을 다시 입력해야 하는 시간을 줄일 수 있으므로 생산성이 향상됩니다.
- 애플리케이션을 호스팅하는 시스템에서 인증을 타사 시스템으로 전송합니다.
- 비밀번호 재설정을 위한 헬프 데스크 호출 건수가 줄어들어 비용이 낮아지므로 더 많은 비용 절감 효과를 거둘 수 있습니다.

IdP는 사용자, 시스템 또는 서비스를 위한 ID 정보를 생성, 유지 및 관리하는 인증 모듈입니다. IdP는 사용자 자격 증명을 저장 및 검증하고, SAML 응답을 생성하므로 사용자는 서비스 제공자에 의해 보호된 리소스에 액세스할 수 있습니다.

참고 관리자는 IdP 서비스에 대해 잘 알고 있어야 하며, 현재 설치되어 작동 중인지 확인해야 합니다.

SAML SSO는 다음 포털에서 지원됩니다.

- 게스트 포털(스폰서 및 셀프 등록)
- 스폰서 포털
- 내 디바이스 포털
- 인증서 프로비저닝 포털

BYOD 포털의 외부 ID 소스로 IdP를 선택할 수 없지만, 게스트 포털에 사용할 IdP를 선택하고 BYOD 플로우를 활성화할 수 있습니다.

Cisco ISE는 SAMLv2를 준수하며 Base64 인코딩 인증서를 사용하는 모든 SAMLv2 준수 IdP를 지원합니다. 아래에는 Cisco ISE에서 테스트된 IdP가 나와 있습니다.

- OAM(Oracle Access Manager)
- OIF(Oracle Identity Federation)
- SecureAuth
- PingOne
- PingFederate
- Azure Active Directory

IdP는 ID 소스 시퀀스에 추가할 수 없습니다.

지정된 시간(기본값은 5분) 동안 활동이 없는 경우 SSO 세션이 종료되고 세션 시간 제한 오류 메시지가 표시됩니다.

포털의 오류 페이지에 Sign On Again(다시 로그인) 버튼을 추가하려면 포털 오류 페이지의 Optional Content(선택적 콘텐츠) 필드에 다음 JavaScript를 추가해 주십시오.

```
<button class="cisco-ise" data-inline="true" data-mini="true" data-theme="b"
id="ui_aup_accept_button" onclick="location.href='PortalSetup.action?portal=<Portal ID>'"
type="button">SignOn Again</button>
```

Cisco ISE에서 SAML ID 제공자 구성

Cisco ISE에서 SAML ID 제공자를 구성하려면,

- Cisco ISE에서 슈퍼 관리자 또는 시스템 관리자여야 합니다.
- IdP(ID 제공자)가 인증서에 셀프 서명을 하지 않은 경우 신뢰할 수 있는 인증서 저장소로 CA(Certificate Authority) 인증서를 가져옵니다.
- 구성중인 IdP 포털에 대한 관리자 액세스 권한이 있어야 합니다. 다음 작업에는 IdP 포털에서 수행해야 하는 몇 가지 단계가 포함되어 있습니다.

Cisco ISE에서 SAML ID 제공자를 구성하려면,

1. Cisco ISE에 SAML ID 제공자를 추가합니다.
2. 포털의 인증 방법으로 SAML ID 제공자를 추가합니다.
3. SAML ID 공급자를 구성합니다.

Cisco ISE에 SAML ID 제공자 추가

단계 **1** **Administration(**관리**)** > **External Identity Sources(**외부 **ID** 소스**)** > **SAML Id Providers(SAML ID** 제공자**)**Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 .

단계 **2** **Add(**추가**)**를 클릭합니다.

단계 **3** 표시된 **SAML Identity Provider(SAML ID** 제공자**)** 창의 **General(**일반**)** 탭에서 **Id Provider Name(ID** 제공자 이름**)** 및 **Description(**설명**)**을 입력합니다.

단계 **4** **Submit(**제출**)**을 클릭합니다.

단계 **5** **Identity Provider Config(ID** 제공자 컨피그레이션**)** 탭에서 관련 메타 데이터 .xml 파일을 가져오고 **Submit(**제출**)**을 클릭합니다.

포털의 인증 방법으로 SAML ID 제공자 추가

방금 생성한 SAML ID 제공자를 다음 포털에 추가할 수 있습니다.

1. 셀프 등록 게스트 포털 및 스폰서 게스트 포털(**Work Centers(**작업 센터**)** > **Guest Access(**게스트 액세스**)** > **Portals and Components(**포털 및 구성 요소**)**)

2. 인증서 프로비저닝 포털(**Administration(**관리**)** > **Device Portal Management(**디바이스 포털 관리**)** > **Certificate Provisioning(**인증서 프로비저닝**)** > **Certificate Provisioning Portal(**인증서 프로비저닝 포털**)**)

단계 **1** 구성중인 포털의 포털 사용자 맞춤화 창에서 **Portal Settings(**포털 설정**)**를 클릭합니다.

단계 **2** 표시되는 드롭 다운 섹션에서 **Authentication Method(**인증 방법**)** 섹션으로 이동하여 메뉴를 사용하여 추가한 SAML IP 제공자를 선택합니다.

단계 **3** **Save(**저장**)**를 클릭합니다.

SAML ID 제공자 구성

단계 **1** **Administration(**관리**)** > **External Identity Sources(**외부 **ID** 소스**)** > **SAML Id Providers(SAML ID** 제공자**)**Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 . 해당 포털에 방금 연결한 IdP를 선택하고 **Edit(**편집**)**를 클릭합니다.

단계 **2** (선택 사항) Cisco ISE 노드의 로드를 최적화하기 위해 로드 밸런서를 사용하는 경우 IdP 구성을 간소화하기 위해 **Service Provider Info(**서비스 제공자 정보**)** 탭에서 세부정보를 추가할 수 있습니다. 소프트웨어 또는 하드웨어 로드 밸런서를 추가할 수 있습니다.

Portal Settings(포털 설정**)** 창에 지정된 포트를 사용하여 로드 밸런서에서 구축 환경의 Cisco ISE 노드로 요청을 전달할 수 있어야 합니다.

로드 밸런서를 추가한 경우에는 서비스 제공자 메타데이터 파일에서 로드 밸런서 URL만 제공됩니다. 로드 밸런서가 없으면 서비스 제공자 메타데이터 파일에 여러 **AssertionConsumerService** URL이 포함됩니다.

참고 포털 FQDN 설정에서 로드 밸런서에 대한 동일한 주소를 사용하지 않는 것이 권장됩니다.

단계 **3** **Service Provider Info(**통신 사업자 정보**)** 탭에서 **Export(**내보내기**)**를 클릭하여 통신 사업자 메타데이터 파일을 내보냅니다. 내보낸 메타데이터에는 Cisco ISE의 서명 인증서가 포함되어 있습니다. 이 서명 인증서는 선택한 포털의 인증서와 동일합니다.

내보낸 메타데이터 zip 폴더에는 각 IdP(Azure Active Directory, PingOne, PingFederate, SecureAuth, OAM 등)를 구성하기 위한 기본적인 지침이 포함된 추가 정보 파일이 들어 있습니다.

다음 사항이 변경된 경우에는 서비스 제공자 메타데이터를 다시 내보내야 합니다.

- 새 Cisco ISE 노드 등록
- 노드의 호스트 이름 또는 IP 주소
- 내 디바이스, 스폰서 또는 인증서 프로비저닝 포털의 FQDN(Fully Qualified Domain Name)
- 포트 또는 인터페이스 설정
- 연결된 로드 밸런서

업데이트된 메타데이터를 다시 내보내지 않으면 IdP 쪽에서 사용자 인증 요청을 거부할 수 있습니다.

단계 **4** IdP 포털로 이동하여 관리자로 로그인한 다음 방금 Cisco ISE에서 내보낸 서비스 제공자 메타데이터 파일을 가져옵니다. 먼저 포털 이름을 사용하여 내보낸 폴더와 메타데이터 파일의 압축을 풀어야 합니다. 메타데이터 파일에는 제공자 ID 및 바인딩 URI가 포함되어 있습니다.

단계 **5** Cisco ISE 포털로 돌아갑니다.

단계 **6** (선택 사항) **SAML Identity Provider(SAML ID** 제공자**)** 창의 **Groups(**그룹**)** 탭에서 필요한 사용자 그룹을 추가합니다.

Group Membership Attribute(그룹 멤버십 속성**)** 필드에 사용자의 그룹 멤버십을 지정하는 어설션 속성을 입력합니다.

단계 **7** (선택 사항) **Attributes(**속성**)** 탭에서 사용자 속성을 추가하여 IdP에서 반환된 어설션에 속성이 표시되는 방식을 지정합니다.

Name in ISE(ISE 내 이름**)** 필드에서 지정하는 이름이 정책 규칙에 표시됩니다.

다음 데이터 유형이 속성에 대해 지원됩니다.

- 문자열
- 정수
- IPv4
- 부울

단계 **8** **Advanced Settings(**고급 설정**)** 탭에서 다음 옵션을 구성합니다.

옵션	설명
ID 속성	표시된 옵션에 대해 라디오 버튼을 클릭하여 인증 중인 사용자의 ID를 지정하는 속성을 선택합니다. 참고 Cisco ISE는 SAML IdP 임시 또는 영구 형식의 주체 이름(NameID)을 포함하는 응답을 지원하지 않습니다. 이러한 방법을 사용할 경우 Cisco ISE는 사용자 이름 속성 어설션을 검색할 수 없으며 인증은 실패하게 됩니다.
이메일 속성	드롭다운 목록에서 사용자의 이메일 주소를 반환하는 어설션 속성을 선택합니다. 스폰서 하나에 대해 승인할 스폰서 게스트 목록을 필터링(제한)하려는 경우 이메일 속성을 구성해야 합니다.
다중 값 속성	다음 중 하나를 선택합니다. • **Each value in a separate XML(**개별 **XML**의 각 값**)**: IdP가 개별 XML 요소에서 속성이 같은 여러 값을 반환하는 경우 이 옵션을 클릭합니다. • **Multiple values in a single XML(**단일 **XML**의 여러 값**)**: IdP가 단일 XML 요소의 여러 값을 반환하는 경우 이 옵션을 클릭합니다. 텍스트 상자에서 구분 기호를 지정합니다.
로그아웃 설정	로그아웃 요청에 서명하려면 **Sign Logout Requests(**로그아웃 요청 서명**)** 확인란을 선택합니다. 구성 중인 IdP가 Oracle Access Manager 또는 Oracle Identity Federation인 경우 이 옵션은 표시되지 않습니다. 참고 SecureAuth에서는 SAML 로그아웃을 지원하지 않습니다.

옵션	설명
	다음 옵션은 Oracle Access Manager 또는 Oracle Identity Federation IdP를 구성하고 로드 밸런서를 구성하지 않은 경우에만 표시됩니다. • **Logout URL(**로그아웃 **URL)**: 사용자가 스폰서 또는 내 디바이스 포털에서 로그아웃할 때 SSO 세션을 종료하도록 리디렉션되는 페이지의 URL을 입력합니다. • **Redirect Parameter Name(**리디렉션 매개변수 이름**)**: SSO 세션이 종료되면 사용자가 IdP의 로그인 페이지로 돌아갑니다. 리디렉션 매개변수 이름은 IdP에 따라 다를 수 있습니다(예: **end_url** 또는 **returnURL**). 이 필드는 대/소문자를 구분합니다. 정상적으로 로그아웃되지 않는 경우 IdP 설명서에서 로그아웃 URL 및 리디렉션 매개변수 이름에 대한 세부정보를 확인하십시오.
인증 상황	이 섹션을 사용하여 SAML IdP 인증 상황 클래스 참조를 편집합니다. Cisco ISE SAML 요청은 일반적으로 SAML 요청 제목에서 **PasswordProtectedTransport** 인증 방법을 사용했습니다. 이로 인해 다중 인증이 사용되는 경우 인증이 실패하게 됩니다. 이를 방지하기 위해 **AuthnContextClassRef SAML Element** 섹션을 사용하여 인증 방법을 지정할 수 있습니다. 사용된 인증 방법을 잘 모를 경우 인증 실패를 방지하기 위해 이 섹션을 비워 두는 것이 좋습니다.

단계 **9** **Submit(**제출**)**을 클릭합니다.

ID 제공자 삭제

시작하기 전에

다음 작업을 수행하려면 슈퍼 관리자 또는 시스템 관리자여야 합니다.

삭제할 IdP가 포털에 연결되어 있지 않은지 확인합니다. IdP가 포털에 연결되어 있으면 삭제 작업이 실패합니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**) > Network Access(**네트워크 액세스**) > Ext Id Sources(**외부 **ID** 소스**) > SAML Id Providers(SAML ID** 제공자**)**를 선택합니다.

단계 **2** 삭제할 IdP 옆의 확인란을 선택하고 **Delete(**삭제**)**를 클릭합니다.

단계 **3** 선택한 IdP를 삭제하려면 **OK(**확인**)**를 클릭합니다.

인증 장애 로그

SAML ID 저장소에 대한 인증에서 장애가 발생하고 IdP가 SAML 응답을 통해 사용자를 다시 ISE 포털로 리디렉션하면 ISE는 인증 로그에 실패 이유를 보고하게 됩니다. 게스트 포털의 경우 BYOD 플

로우 활성화 여부에 관계없이 RADIUS 라이브 로그를 확인(Operations(운영) > RADIUS > Live Log(라이브 로그))하여 인증 실패 이유를 확인할 수 있습니다. 내 디바이스 포털 및 스폰서 포털의 경우 내 디바이스 로그인/감사 보고서 및 스폰서 로그인/감사 보고서를 확인(Operations(운영) > Reports(보고서) > Guest(게스트))하여 인증 실패 이유를 확인할 수 있습니다.

로그아웃 장애 발생 시 보고서와 로그를 확인하여 내 디바이스, 스폰서 및 게스트 포털에 대한 실패 이유를 확인할 수 있습니다.

인증은 다음과 같은 이유로 실패할 수 있습니다.

- SAML 응답 구문 분석 오류
- SAML 응답 검증 오류(예: 잘못된 발급자)
- SAML 어설션 검증 오류(예: 잘못된 대상)
- SAML 응답 서명 검증 오류(예: 잘못된 서명)
- IdP 인증서 서명 오류(예: 인증서 취소됨)

참고 Cisco ISE는 암호화된 어설션을 사용하는 SAML 응답을 지원하지 않습니다. IdP에서 이 기능이 구성된 경우 ISE에 다음 오류 메시지가 표시됩니다. `FailureReason=24803 Unable to find 'username' attribute assertion.`

인증이 실패하는 경우 인증 로그에서 "DetailedInfo" 속성을 확인하는 것이 좋습니다. 이 속성은 실패 원인에 대한 추가 정보를 제공합니다.

ID 소스 시퀀스

ID 소스 시퀀스는 Cisco ISE가 여러 데이터베이스에서 사용자 자격 증명을 찾는 순서를 정의합니다.

Cisco ISE에 연결된 여러 데이터베이스에 사용자 정보가 있는 경우 Cisco ISE가 이러한 ID 소스에서 정보를 찾는 순서를 정의할 수 있습니다. 일치 항목이 발견되면 Cisco ISE는 추가로 검색하지 않고 자격 증명을 평가한 후 사용자에게 결과를 반환합니다. 이는 처음 일치 정책입니다.

ID 소스 시퀀스 생성

시작하기 전에

Cisco ISE에서 외부 ID 소스를 구성했는지 확인합니다.

다음 작업을 수행하려면 슈퍼 관리자 또는 시스템 관리자여야 합니다.

게스트 사용자가 로컬 WebAuth를 통해 인증하도록 허용하려면 게스트 포털 인증 소스와 ID 소스 시퀀스가 동일한 ID 저장소를 포함하도록 구성해야 합니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **Identity Source Sequences(ID** 소스 시퀀스**)** > **Add(**추가**)**를 선택합니다.

단계 **2** ID 소스 시퀀스의 이름을 입력합니다. 원하는 경우 설명을 입력할 수도 있습니다.

단계 **3** **Select Certificate Authentication Profile(**인증서 인증 프로파일 선택**)** 확인란을 선택하고 인증서 기반 인증용 인증서 인증 프로파일을 선택합니다.

단계 **4** ID 소스 시퀀스에 포함할 하나 이상의 데이터베이스를 **Selected List(**선택됨 목록**)** 필드에서 선택합니다.

단계 **5** Cisco ISE가 데이터베이스를 검색하도록 할 순서대로 **Selected List(**선택됨 목록**)** 필드의 데이터베이스를 다시 정렬합니다.

단계 **6** **Advanced Search List(**고급 검색 목록**)** 영역에서 다음 옵션 중 하나를 선택합니다.

- **Do not access other stores in the sequence and set the AuthenticationStatus attribute to ProcessError(**시퀀스의 다른 저장소에 액세스하지 않고 **AuthenticationStatus** 속성을 **ProcessError**로 설정**)**: 처음 선택한 ID 소스에서 사용자를 찾을 수 없는 경우 Cisco ISE가 검색을 중지하도록 하려면 이 옵션을 선택합니다.
- **Treat as if the user was not found and proceed to the next store in the sequence(**사용자를 찾지 못한 것으로 간주하여 다음 저장소로 순차 진행**)**: 처음 선택한 ID 소스에서 사용자를 찾을 수 없는 경우 Cisco ISE가 시퀀스에서 선택한 다른 ID 소스에서 검색을 계속하도록 하려면 이 옵션을 선택합니다.

  요청을 처리하는 동안 Cisco ISE는 이러한 ID 소스를 순서대로 검색합니다. Selected list(선택됨 목록) 필드의 ID 소스가 Cisco ISE가 검색하도록 할 순서대로 나열되어 있는지 확인합니다.

단계 **7** ID 소스 시퀀스를 생성하려면 **Submit(**제출**)**을 클릭합니다. 생성된 시퀀스는 정책에서 사용할 수 있습니다.

ID 소스 시퀀스 삭제

정책에서 더 이상 사용하지 않는 ID 소스 시퀀스를 삭제할 수 있습니다.

시작하기 전에

- 삭제하려는 ID 소스 시퀀스가 인증 정책에서 사용되지 않는지 확인합니다.
- 다음 작업을 수행하려면 슈퍼 관리자 또는 시스템 관리자여야 합니다.

단계 **1** **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **Identity Source Sequences(ID** 소스 시퀀스**)**를 선택합니다.

단계 **2** 삭제할 하나 이상의 ID 소스 시퀀스 옆에 있는 확인란을 선택하고 **Delete(**삭제**)**를 클릭합니다.

단계 **3** **OK(**확인**)**를 클릭하여 하나 이상의 ID 소스 시퀀스를 삭제합니다.

보고서의 ID 소스 세부정보

Cisco ISE는 인증 dashlet 및 ID 소스 보고서에서 ID 소스에 대한 정보를 제공합니다.

인증 Dashlet

인증 dashlet에서 실패 이유를 비롯한 추가 정보를 드릴다운할 수 있습니다.

실시간 인증 요약을 확인하려면 Operations(작업) > RADIUS Livelog(RADIUS 라이브 로그)를 선택합니다. RADIUS 라이브 로그에 대한 자세한 내용은 RADIUS 라이브 로그을 참고하십시오.

ID 소스 보고서

Cisco ISE는 ID 소스에 대한 정보가 포함된 다양한 보고서를 제공합니다. 이러한 보고서에 대한 설명은 사용 가능한 보고서 섹션을 참고해 주십시오.

네트워크에서 프로파일링된 엔드포인트

프로파일러 서비스는 디바이스 유형에 관계없이 네트워크의 모든 엔드포인트 기능(Cisco ISE에서 ID라고 함)을 식별하고 찾고 확인하는 데 도움이 됩니다. 이를 통해 엔터프라이즈 네트워크에 적절하게 액세스하는지 확인하고 이러한 액세스를 유지 관리할 수 있습니다. Cisco ISE 프로파일러 기능은 여러 프로브를 사용하여 네트워크의 모든 엔드포인트에 대한 속성을 수집하고 이를 프로파일러 분석기로 전달합니다. 여기서 알려진 엔드포인트는 연결된 정책 및 ID 그룹에 따라 분류됩니다.

Cisco ISE에서 프로파일러 피드 서비스를 사용하는 관리자는 지정된 Cisco 피드 서버에서 서브스크립션을 통해 신규 및 업데이트된 엔드포인트 프로파일링 정책 및 업데이트된 OUI 데이터베이스를 피드로 가져올 수 있습니다.

프로파일러 조건 설정

다음 표에서는 프로파일러 조건 창의 필드에 대해 설명합니다. 이 창의 탐색 경로는 **Policy(정책)** > **Policy Elements(정책 요소)** > **Conditions(조건)** > **Profiling(프로파일링)**입니다.

표 ***41:*** 프로파일러 조건 설정

필드 이름	사용 지침
Name(이름)	프로파일러 조건의 이름입니다.
Description(설명)	프로파일러 조건의 설명입니다.
Type(유형)	미리 정의된 유형 중 하나를 선택합니다.

필드 이름	사용 지침
Attribute Name(속성 이름)	프로파일러 조건의 기준으로 사용할 속성을 선택합니다.
Operator(연산자)	연산자를 선택합니다.
Attribute Value(속성 값)	선택한 속성에 대한 값을 입력합니다. 미리 정의된 속성 값을 포함하는 속성 이름의 경우 이 옵션에는 미리 정의된 값이 포함된 드롭다운 목록이 표시되며, 이 목록에서 값을 선택할 수 있습니다.
System Type(시스템 유형)	프로파일링 조건은 다음 유형 중 하나일 수 있습니다. • **Cisco** 제공: 구축 시 Cisco ISE에서 제공되는 프로파일링 조건은 Cisco 제공으로 식별됩니다. 이러한 조건은 시스템에서 삭제하거나 편집할 수 없습니다. • 관리자 생성: Cisco ISE의 관리자가 생성하는 프로파일링 조건은 관리자 생성으로 식별됩니다.

관련 항목

Cisco ISE 프로파일링 서비스, 186 페이지
프로파일러 조건, 214 페이지
프로파일러 피드 서비스, 256 페이지
프로파일러 조건 생성, 230 페이지

Cisco ISE 프로파일링 서비스

Cisco ISE(Identity Services Engine)의 프로파일링 서비스는 네트워크에 연결되는 디바이스와 해당 위치를 식별합니다. 엔드포인트는 Cisco ISE에서 구성한 엔드포인트 프로파일링 정책에 따라 프로파일링됩니다. 그런 다음 Cisco ISE는 정책 평가 결과를 기준으로 네트워크의 리소스에 액세스할 수 있는 권한을 엔드포인트에 부여합니다.

프로파일링 서비스:

- 다양한 규모와 복잡성을 지닌 모든 엔터프라이즈 네트워크에 IEEE 표준 802.1X 포트 기반 인증 액세스 제어, MAB(MAC Authentication Bypass) 인증 및 NAC(Network Admission Control)를 사용하여 효율적이고 효과적인 구축과 지속적인 인증 관리를 촉진합니다.
- 엔드포인트 유형에 관계없이 연결된 모든 네트워크 엔드포인트의 기능을 식별하거나 찾고 결정합니다.
- 일부 엔드포인트에 대한 액세스를 실수로 거부하지 못하게 보호합니다.

ISE 커뮤니티 리소스

ISE 엔드포인트 프로파일

방법: ISE 프로파일링 설계 가이드

프로파일러 작업 센터

프로파일러 작업 센터 메뉴(Work Centers[작업 센터] > Profiler[프로파일러])에는 ISE 관리자에게 단일 시작점 역할을 하는 모든 프로파일러 페이지가 포함되어 있습니다. 프로파일러 작업 센터 메뉴에는 Overview(개요), Ext ID Stores(외부 ID 저장소), Network Devices(네트워크 디바이스), Endpoint Classification(엔드포인트 분류), Node Config(노드 컨피그레이션), Feeds(피드), Manual Scans(수동 스캔), Policy Elements(정책 요소), Profiling Policies(프로파일링 정책), Authorization Policy(권한 부여 정책), Troubleshoot(문제 해결), Reports(보고서), Settings(설정) 및 Dictionaries(사전) 옵션이 포함되어 있습니다.

프로파일러 대시보드

프로파일러 대시보드(Work Centers[작업 센터] > Profiler[프로파일러] > Endpoint Classification[엔드포인트 분류])는 네트워크의 프로파일, 엔드포인트 및 자산용 중앙 집중식 모니터링 툴입니다. 대시보드에는 데이터가 그래픽 및 표 형식으로 표시됩니다. 프로파일 대시릿에는 네트워크에서 현재 활성 상태인 논리 프로파일과 엔드포인트 프로파일이 표시됩니다. 엔드포인트 대시릿에는 네트워크에 연결하는 엔드포인트의 ID 그룹, PSN 및 OS 유형이 표시됩니다. 자산 대시릿에는 Guest(게스트), BYOD, Corporate(기업) 등의 플로우가 표시됩니다. 표에는 연결된 다양한 엔드포인트가 표시되며, 새 엔드포인트를 추가할 수도 있습니다.

프로파일링 서비스를 사용하는 엔드포인트 인벤토리

프로파일링 서비스를 사용하여 네트워크에 연결된 모든 엔드포인트의 기능을 검색하고 찾고 확인할 수 있습니다. 그러면 디바이스 유형에 관계없이 엔드포인트가 엔터프라이즈 네트워크에 적절하게 액세스하는지 확인하고 이러한 액세스를 유지 관리할 수 있습니다.

프로파일링 서비스는 네트워크 디바이스와 네트워크에서 엔드포인트의 속성을 수집하고, 프로파일에 따라 엔드포인트를 특정 그룹으로 분류하고, 일치하는 프로파일과 함께 엔드포인트를 Cisco ISE 데이터베이스에 저장합니다. 프로파일링 서비스가 처리하는 모든 속성을 프로파일러 사전에서 정의해야 합니다.

프로파일링 서비스는 네트워크의 각 엔드포인트를 식별한 다음 프로파일에 따라 이러한 엔드포인트를 시스템의 기존 엔드포인트 ID 그룹이나 시스템에서 생성할 수 있는 새 그룹으로 그룹화합니다. 이와 같이 엔드포인트를 그룹화하고 엔드포인트 ID 그룹에 엔드포인트 프로파일링 정책을 적용하면 해당하는 엔드포인트 프로파일링 정책에 대한 엔드포인트의 매핑을 결정할 수 있습니다.

Cisco ISE 프로파일러 큐 제한 컨피그레이션

Cisco ISE 프로파일러는 짧은 시간 동안 네트워크에서 막대한 양의 엔드포인트 데이터를 수집합니다. 따라서 일부 느려진 Cisco ISE 구성 요소가 프로파일러에서 생성된 데이터를 처리할 때 누적된 백로그로 인해 JVM(Java Virtual Machine) 메모리 사용률이 높아지고 결과적으로 성능 저하 및 안정성 문제가 발생할 수 있습니다.

프로파일러에서 JVM 메모리 사용률이 증가하지 않고 JVM의 메모리가 부족해져 다시 시작되는 것을 방지하기 위해 프로파일러의 다음 내부 구성 요소에 제한이 적용됩니다.

- 엔드포인트 캐시: 크기가 제한을 초과하는 경우 주기적으로 (가장 최근에 사용한 전략에 따라) 제거되도록 내부 캐시의 크기가 제한됩니다.
- 전달자: 프로파일러에서 수집되는 엔드포인트 정보의 기본 인그레스 큐입니다.
- 이벤트 처리기: 느린 처리 구성 요소(일반적으로 데이터베이스 쿼리 관련)에 데이터를 공급하는 빠른 구성 요소의 연결을 끊는 내부 큐입니다.

엔드포인트 캐시

- maxEndPointsInLocalDb = 100000(캐시의 엔드포인트 객체)
- endPointsPurgeIntervalSec = 300(초당 엔드포인트 캐시 제거 스레드 간격)
- numberOfProfilingThreads = 8(스레드 수)

이 제한은 모든 프로파일러 내부 이벤트 처리기에 적용됩니다. 큐 크기 제한에 도달하면 모니터링 경보가 트리거됩니다.

Cisco ISE 프로파일러 큐 크기 제한

- forwarderQueueSize = 5000(엔드포인트 수집 이벤트)
- eventHandlerQueueSize = 10000(이벤트)

이벤트 처리기

- NetworkDeviceEventHandler: 이미 캐시된 중복 NAD(Network Access Device) IP 주소 필터링 외에 네트워크 디바이스 이벤트에 사용
- ARPCacheEventHandler: ARP 캐시 이벤트에 사용

화성 IP 주소

RADIUS 구문 분석기가 프로파일링 서비스에 도달하기 전에 화성 IP 주소를 제거하므로 해당 주소는 **Context Visibility(**상황 가시성**)** > **Endpoints(**엔드포인트**)** 및 **Work Centers(**작업 센터**)** > **Profiler(**프로파일러**)** > **Endpoint Classification(**엔드포인트 분류**)**창에 표시되지 않습니다. 화성 IP 주소는 공격에 취약하기 때문에 보안 문제가 됩니다. 그러나 화성 IP 주소는 감사 목적으로 MnT 로그에 표시됩니다. 이 동작은 멀티캐스트 IP 주소의 경우에도 마찬가지입니다. 화성 IP 주소에 대한 자세한 내용은

https://www.cisco.com/assets/sol/sb/Switches_Emulators_v2_3_5_xx/help/250/index.html#page/tesla_250_olh/martian_addresses.html을 참조하십시오.

프로파일러 전환 지속성 대기열

프로파일러 전환 지속성 대기열은 프로파일러 모듈로 전송되기 전에 추후 처리에 사용할 수 있도록 이벤트를 저장합니다. 또한 증가된 이벤트 처리를 지원하기 위해 대기열에 저장 가능한 용량도 늘어났습니다. 이렇게 하면 이벤트 수가 갑자기 증가하여 손실되는 이벤트 수가 감소하게 됩니다. 대기열이 최대 한도에 도달하면 경보가 줄어듭니다.

이 기능은 기본적으로 활성화되어 있습니다. 필요한 경우 해당 기능을 비활성화하여 이벤트가 프로파일러 모듈로 직접 전송되는 원래 메커니즘으로 대체할 수 있습니다. 이 기능을 활성화하거나 비활성화하려면 **Administration(**관리**)** > **System(**시스템**)** > **Settings(**설정**)** > **Profiling(**프로파일링**)**을 선택하고 **Enable Profiler Forwarder Persistence Queue(**프로파일러 전환 지속성 대기열**)** 확인란을 선택하거나 선택 취소합니다.

Cisco ISE 노드에서 프로파일링 서비스 구성

Cisco ISE가 활성화된 네트워크에서 네트워크 리소스를 사용하는 모든 엔드포인트의 상황별 인벤토리를 제공하는 프로파일링 서비스를 구성할 수 있습니다.

기본적으로 관리, 모니터링 및 정책 서비스 페르소나 역할을 모두 수행하는 단일 Cisco ISE 노드에서 실행되도록 프로파일링 서비스를 구성할 수 있습니다.

분산형 구축에서 프로파일링 서비스는 정책 서비스 페르소나 역할을 하는 Cisco ISE 노드에서만 실행되며, 관리 및 모니터링 페르소나 역할을 하는 기타 Cisco ISE 노드에서는 실행되지 않습니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Deployment(**구축**)**를 선택합니다.

단계 **2** 정책 서비스 페르소나 역할을 하는 Cisco ISE 노드를 선택합니다.

단계 **3** 구축 노드 페이지에서 **Edit(**편집**)**를 클릭합니다.

단계 **4** **General Settings(**일반 설정**)** 탭에서 **Policy Service(**정책 서비스**)** 확인란을 선택합니다. Policy Service(정책 서비스) 확인란 선택을 취소하면 세션 서비스와 프로파일링 서비스 확인란이 모두 비활성화됩니다.

단계 **5** 다음 작업을 수행합니다.

a) 네트워크 액세스, 포스처, 게스트 및 클라이언트 프로비저닝 세션 서비스를 실행하려면 **Enable Session Services(**세션 서비스 활성화**)** 확인란을 선택합니다.

b) 프로파일링 서비스를 실행하려면 **Enable Profiling Services(**프로파일링 서비스 활성화**)** 확인란을 선택합니다.

c) 디바이스 관리 서비스를 실행하여 기업의 네트워크 디바이스를 제어하고 감사하려면 **Enable Device Admin Service(**디바이스 관리 서비스 활성화**)** 확인란을 선택합니다.

단계 **6** **Save(**저장**)**를 클릭하여 노드 컨피그레이션을 저장합니다.

프로파일링 서비스에 사용되는 네트워크 프로브

네트워크 프로브는 네트워크의 엔드포인트에서 속성 또는 속성 집합을 수집하는데 사용되는 방법입니다. 프로브를 사용하면 엔드포인트를 생성하거나 Cisco ISE 데이터베이스에서 엔드포인트와 일치하는 프로파일로 엔드포인트를 업데이트할 수 있습니다.

Cisco ISE는 네트워크의 디바이스 동작을 분석하고 디바이스 유형을 확인하는 여러 네트워크 프로브를 사용하여 디바이스를 프로파일링할 수 있습니다. 네트워크 프로브는 네트워크를 보다 효과적으로 파악하도록 도와줍니다.

IP 주소와 MAC 주소 바인딩

엔터프라이즈 네트워크에서 엔드포인트의 MAC 주소를 사용하는 방법으로만 엔드포인트를 생성하거나 업데이트할 수 있습니다. ARP 캐시에서 엔트리를 찾을 수 없으면 Cisco ISE에서 NetFlow 패킷의 IN_SRC_MAC 및 HTTP 패킷의 L2 MAC 주소를 사용하여 엔드포인트를 생성하거나 업데이트할 수 있습니다. 엔드포인트가 1홉 거리에 있을 때는 L2 인접도에 따라 프로파일링 서비스가 달라집니다. 엔드포인트가 L2에 인접해 있으면 엔드포인트의 IP 주소와 MAC 주소는 이미 매핑되어 있으므로 IP-MAC 캐시 매핑을 수행할 필요가 없습니다.

엔드포인트가 L2에 인접해 있지 않으며 여러 홉 거리에 있으면 매핑이 안정적으로 수행되지 않을 수 있습니다. 수집하는 NetFlow 패킷의 알려진 속성으로는 PROTOCOL, L4_SRC_PORT, IPV4_SRC_ADDR, L4_DST_PORT, IPV4_DST_ADDR, IN_SRC_MAC, OUT_DST_MAC, IN_SRC_MAC, OUT_SRC_MAC 등이 있습니다. 엔드포인트가 L2에 인접해 있지 않으며 여러 L3 홉 거리에 있으면 IN_SRC_MAC 속성은 L3 네트워크 디바이스의 MAC 주소만 전달합니다. Cisco ISE에서 HTTP 프로브가 활성화되어 있으면 HTTP 패킷의 MAC 주소를 사용하는 방법으로만 엔드포인트를 생성할 수 있습니다. HTTP 요청 메시지가 페이로드 데이터에서 엔드포인트의 IP 주소 및 MAC 주소를 전달하지 않기 때문입니다.

엔드포인트의 IP 주소와 MAC 주소를 안정적으로 매핑할 수 있도록 Cisco ISE는 프로파일링 서비스에서 ARP 캐시를 구현합니다. ARP 기능이 작동하려면 DHCP 프로브 또는 RADIUS 프로브를 활성화해야 합니다. DHCP 및 RADIUS 프로브는 페이로드 데이터에서 엔드포인트의 IP 주소 및 MAC 주소를 전달합니다. DHCP 프로브의 dhcp-requested address 속성과 RADIUS 프로브의 Framed-IP-address 속성은 엔드포인트의 IP 주소를 해당 MAP 주소와 함께 전달하며, 이 IP 주소를 매핑하여 ARP 캐시에 저장할 수 있습니다.

NetFlow 프로브

Cisco ISE 프로파일러는 Cisco IOS NetFlow 버전 9를 구현합니다. Cisco ISE 프로파일링 서비스를 지원하기 위해 프로파일러를 개선하는 데 필요한 추가 기능이 포함되어 있는 NetFlow 버전 9를 사용하는 것이 좋습니다.

NetFlow가 활성화된 네트워크 액세스 디바이스에서 NetFlow 버전 9 속성을 수집하여 엔드포인트를 생성하거나 Cisco ISE 데이터베이스의 기존 엔드포인트를 업데이트할 수 있습니다. 엔드포인트의 소스 및 대상 MAC 주소를 연결하고 업데이트하도록 NetFlow 버전 9를 구성할 수 있습니다. 또한 NetFlow 기반 프로파일링을 지원하기 위해 NetFlow 속성 사전을 생성할 수도 있습니다.

NetFlow 버전 9 기록 형식에 대한 자세한 내용은 NetFlow 버전 9 흐름 기록 형식 문서의 표 6 "NetFlow 버전 9 필트 유형 정의"를 참고해 주십시오.

Cisco ISE는 버전 5 이전의 NetFlow 버전도 지원합니다. 네트워크에서 NetFlow 버전 5를 사용하는 경우, 다른 위치에서는 해당 버전이 작동하지 않으므로 액세스 레이어의 기본 NAD(Network Access Device)에서만 버전 5를 사용할 수 있습니다.

Cisco IOS NetFlow 버전 5 패킷은 엔드포인트의 MAC 주소를 포함하지 않습니다. NetFlow 버전 5에서 수집된 속성을 Cisco ISE 데이터베이스에 직접 추가할 수는 없습니다. IP 주소를 사용하여 엔드포인트를 검색하고 NetFlow 버전 5 속성을 엔드포인트에 추가할 수 있습니다. 이렇게 하려면 네트워크 액세스 디바이스의 IP 주소와 NetFlow 버전 5 속성에서 가져온 IP 주소를 결합합니다. 단, 이렇게 하려면 RADIUS 또는 SNMP 프로브를 사용하여 이러한 엔드포인트를 이전에 검색한 상태여야 합니다.

NetFlow 버전 5 이전의 버전에서는 MAC 주소가 IP 흐름의 일부분이 아니므로 엔드포인트 캐시에서 네트워크 액세스 디바이스로부터 수집한 속성 정보의 상관관계를 지정하여 IP 주소로 엔드포인트를 프로파일링해야 합니다.

NetFlow 버전 5 기록 형식에 대한 자세한 내용은 NetFlow 서비스 솔루션 설명서의 표 2 "Cisco ISO NetFlow 흐름 기록 및 내보내기 형식 콘텐츠 정보"를 참고해 주십시오.

DHCP 프로브

Cisco ISE 구축의 DHCP(Dynamic Host Configuration Protocol) 프로브를 사용하면 Cisco ISE 프로파일링 서비스에서 INIT-REBOOT 및 SELECTING 메시지 유형의 새 요청만을 기반으로 엔드포인트를 다시 프로파일링할 수 있습니다. RENEWING 및 REBINDING와 같은 다른 DHCP 메시지 유형도 처리되지만 프로파일링 엔드포인트에는 사용하지 않습니다. DHCP 패킷에서 구문 분석되는 속성은 엔드포인트 속성에 매핑됩니다.

INIT-REBOOT 상태에서 생성되는 **DHCPREQUEST** 메시지

DHCP 클라이언트가 이전에 할당 및 캐시된 컨피그레이션을 확인하는 경우 클라이언트는 서버 식별자(server-ip) 옵션을 채워서는 안 됩니다. 대신, 요청된 IP 주소(requested-ip) 옵션을 이전에 할당된 IP 주소로 채우고 DHCPREQUEST 메시지의 클라이언트 IP 주소(ciaddr) 필드를 0으로 채워야 합니다. 그러면 요청된 IP 주소가 잘못되었거나 클라이언트가 잘못된 네트워크에 있는 경우 DHCP 서버가 DHCPNAK 메시지를 클라이언트로 보냅니다.

SELECTING 상태에서 생성되는 **DHCPREQUEST** 메시지

DHCP 클라이언트는 선택한 DHCP 서버의 IP 주소를 서버 식별자(server-ip) 옵션에 삽입하고, 요청된 IP 주소(requested-ip) 옵션을 클라이언트가 선택한 DHCPOFFER의 IP 주소(yiaddr) 필드 값으로 채우고, "ciaddr" 필드를 0으로 채웁니다.

표 ***42:*** 여러 상태의 ***DHCP*** 클라이언트 메시지

—	**INIT-REBOOT**	**SELECTING**	**RENEWING**	**REBINDING**
broadcast/unicast	broadcast	broadcast	unicast	broadcast
server-ip	MUST NOT	MUST	MUST NOT	MUST NOT

—	INIT-REBOOT	SELECTING	RENEWING	REBINDING
requested-ip	MUST	MUST	MUST NOT	MUST NOT
ciaddr	zero	zero	IP address	IP address

DHCP 브리징 모드의 Wireless LAN Controller 컨피그레이션

무선 클라이언트에서 Cisco ISE로 모든 DHCP(Dynamic Host Configuration Protocol) 패킷을 전달할 수 있는 DHCP 브리징 모드에서 WLC(Wireless LAN Controller)를 구성하는 것이 좋습니다. WLC 웹 인터페이스 **Controller(**컨트롤러**)** > **Advanced(**고급**)** > **DHCP Master Controller Mode(DHCP** 마스터 컨트롤러 모드**)** > **DHCP Parameters(DHCP** 매개변수**)**에서 사용 가능한 Enable DHCP Proxy(DHCP 프록시 활성화) 확인란의 선택을 취소해야 합니다. 또한 DHCP IP 헬퍼 명령이 Cisco ISE 정책 서비스 노드를 가리키는지도 확인해야 합니다.

DHCP SPAN 프로브

Cisco ISE 노드에서 초기화된 DHCP SPAN(Switched Port Analyzer) 프로브는 네트워크 액세스 디바이스의 특정 인터페이스에서 들어오는 네트워크 트래픽을 수신 대기합니다. DHCP 서버에서 오는 DHCP SPAN 패킷을 Cisco ISE 프로파일러로 전달하도록 네트워크 액세스 디바이스를 구성해야 합니다. 프로파일러는 이러한 DHCP SPAN 패킷을 받고 구문 분석하여 엔드포인트의 속성을 캡처합니다. 이러한 속성은 프로파일링 엔드포인트에 사용할 수 있습니다.

예:

```
switch(config)# monitor session 1 source interface Gi1/0/4
switch(config)# monitor session 1 destination interface Gi1/0/2
```

HTTP 프로브

HTTP 프로브에서는 ID 문자열이 HTTP request-header 필드 사용자 에이전트로 전송됩니다. 이 문자열은 IP 유형의 프로파일링 조건을 생성하고 웹 브라우저 정보를 확인하는 데 사용할 수 있는 속성입니다. 프로파일러는 요청 메시지의 다른 HTTP 속성과 함께 사용자 에이전트 속성의 웹 브라우저 정보를 캡처한 다음 엔드포인트 속성 목록에 추가합니다.

Cisco ISE는 포트 80과 8080 둘 다에서 웹 브라우저로부터의 통신을 수신 대기합니다. Cisco ISE는 사용자 에이전트 속성을 기준으로 하여 엔드포인트를 식별하도록 시스템에 내장되어 있는 여러 기본 프로파일을 제공합니다.

HTTP 프로브는 기본적으로 활성화되어 있습니다. CWA, 핫스팟, BYOD, MDM 및 Posture와 같은 여러 ISE 서비스는 클라이언트 웹 브라우저의 URL 리디렉션을 사용합니다. 리디렉션된 트래픽에는 연결된 엔드포인트의 RADIUS 세션 ID가 포함됩니다. PSN이 이러한 URL 리디렉션 플로우를 종료하면 암호 해독된 HTTPS 데이터를 확인할 수 있습니다. HTTP 프로브가 PSN에서 비활성화된 경우에도 노드는 웹 트래픽에서 브라우저 사용자 에이전트 문자열을 구문 분석하고 연결된 세션 ID를 기반으로 데이터를 엔드포인트에 연결합니다. 이 방법을 통해 브라우저 문자열이 수집되면 데이터 소스가 HTTP 프로브가 아닌 게스트 포털 또는 CP(Client Provisioning)로 나열됩니다.

HTTP SPAN 프로브

Cisco ISE 구축의 HTTP 프로브를 SPAN(Switched Port Analyzer) 프로브와 함께 활성화하는 경우 프로파일러가 지정된 인터페이스에서 HTTP 패킷을 캡처할 수 있습니다. Cisco ISE가 웹 브라우저로부터의 통신을 수신 대기하는 포트 80에서 SPAN 기능을 사용할 수 있습니다.

HTTP SPAN에서는 IP 헤더(L3 헤더)의 IP 주소와 함께 HTTP 요청 헤더 메시지의 HTTP 속성을 수집합니다. L2 헤더의 엔드포인트 MAC 주소를 기준으로 하여 이 IP 주소를 엔드포인트에 연결할 수 있습니다. 이 정보는 운영체제가 각기 다른 컴퓨터와 Apple 디바이스 등의 여러 모바일 및 휴대용 IP 활성화 디바이스를 식별하는 데 유용합니다. Cisco ISE 서버는 게스트 로그인 또는 클라이언트 프로비저닝 다운로드 중에 캡처를 리디렉션하므로, 여러 모바일 및 휴대용 IP 활성화 디바이스를 보다 안정적으로 식별할 수 있습니다. 따라서 프로파일러가 요청 메시지에서 User-Agent 속성 및 기타 HTTP 속성을 수집한 다음 Apple 디바이스 등의 디바이스를 식별할 수 있습니다.

VMware에서 실행되는 Cisco ISE의 HTTP 속성을 수집할 수 없음

ESX 서버(VMware)에서 Cisco ISE를 구축하는 경우 Cisco ISE 프로파일러는 Dynamic Host Configuration Protocol 트래픽은 수집하지만 vSphere 클라이언트의 컨피그레이션 문제로 인해 HTTP 트래픽은 수집하지 않습니다. VMware 설정에서 HTTP 트래픽을 수집하려면 Cisco ISE 프로파일러에 대해 생성하는 가상 스위치의 Promiscuous Mode(무차별 모드)를 Accept(수락)에서 기본값인 Reject(거부)로 변경하여 보안 설정을 구성합니다. DHCP 및 HTTP의 SPAN(Switched Port Analyzer) 프로브가 활성화되어 있으면 Cisco ISE 프로파일러는 DHCP 및 HTTP 트래픽을 모두 수집합니다.

pxGrid 프로브

pxGrid 프로브는 외부 소스에서 엔드포인트 상황을 수신하기 위해 Cisco pxGrid를 활용합니다. Cisco ISE 2.4 이전에는 Cisco ISE가 게시자로만 사용되었으며 세션 ID 및 그룹 정보와 같은 다양한 상황 정보와 컨피그레이션 요소를 외부 가입자와 공유했습니다. Cisco ISE 2.4에 pxGrid 프로브가 도입됨에 따라 다른 솔루션도 게시자로 사용되며 Cisco ISE 정책 서비스 노드가 가입자가 됩니다.

pxGrid 프로브는 서비스 이름 *com.cisco.endpoint.asset*의 엔드포인트 자산 항목 */topic/com.cisco.endpoint.asset*를 사용하는 pxGrid v2 사양을 기반으로 합니다. 다음 표에는 접두사 자산을 갖는 모든 항목 속성이 표시됩니다.

표 ***43:*** 엔드포인트 자산 항목

속성 이름	**Type(**유형**)**	**Description(**설명**)**
자산 **ID**	길게	자산 ID
자산 이름	문자열	자산 이름
자산 **IP** 주소	문자열	IP 주소
자산 **Mac** 주소	문자열	MAC 주소
자산 벤더	문자열	Manufacturer
자산 제품 **ID**	문자열	제품 코드

자산 일련 번호	문자열	일련 번호
자산 디바이스 유형	문자열	디바이스 유형
자산 **SwRevision**	문자열	S/W 개정 번호
assetHwRevision	문자열	H/W 개정 번호
assetProtocol	문자열	프로토콜
assetConnectedLinks	어레이	네트워크 링크 개체의 어레이
assetCustomAttributes	어레이	맞춤형 이름-값 쌍 어레이

디바이스 MAC 주소(assetMacAddress) 및 IP 주소(assetIpAddress)와 같이 네트워크 자산을 추적하는 데 일반적으로 사용되는 속성 외에도 벤더는 고유 한 엔드포인트 정보를 맞춤형 속성(assetCustomAttributes)으로 게시할 수 있습니다. Cisco ISE에서 엔드포인트 사용자 맞춤화 속성을 사용하면 pxGrid를 통해 공유되는 고유한 각 벤더 속성 집합에 대한 스키마 업데이트 없이도 다양한 활용 사례로 항목을 확장할 수 있습니다.

RADIUS 프로브

RADIUS에 대한 인증을 수행하도록 Cisco ISE를 구성할 수 있습니다. 이때 클라이언트-서버 트랜잭션에 사용 가능한 공유 암호를 정의할 수 있습니다. 프로파일러는 RADIUS 서버에서 수신되는 RADIUS 요청 및 응답 메시지를 사용하여 RADIUS 속성을 수집할 수 있으며, 이러한 속성을 엔드포인트 프로파일링에 사용할 수 있습니다.

Cisco ISE는 RADIUS 서버로 작동할 수 있으며 다른 RADIUS 서버에 대한 RADIUS 프록시 클라이언트로도 작동할 수 있습니다. Cisco ISE는 프록시 클라이언트로 작동할 때 외부 RADIUS 서버를 사용하여 RADIUS 요청 및 응답 메시지를 처리합니다.

RADIUS 프로브는 디바이스 센서에 의해 RADIUS 계정 관리 패킷에서 전송된 속성도 수집합니다. 자세한 내용은 IOS 센서 내장 스위치에서의 속성 수집, 208 페이지 및 IOS 센서 지원 네트워크 액세스 디바이스의 컨피그레이션 체크리스트, 209 페이지를 참조하십시오.

RADIUS 프로브는 기본적으로 실행되며, ISE가 상황 가시성 서비스에 사용하기 위해 엔드포인트 인증 및 권한 부여 세부정보를 추적할 수 있도록 프로파일링 서비스가 구성되지 않은 시스템에서도 마찬가지로 실행됩니다. RADIUS 프로브 및 프로파일링 서비스는 제거 작업을 위해 등록된 엔드포인트의 생성 및 업데이트 시간을 추적하는 데에도 사용됩니다.

표 ***44: RADIUS*** 프로브를 사용하여 수집되는 일반적인 속성

User-Name	**Calling-Station-Id**	**Called-Station-Id**	**Framed-IP-Address**
NAS-IP-Address	NAS-Port-Type	NAS-Port-Id	NAS-Identifier
디바이스 유형(NAD)	위치(NAD)	인증 정책	권한 부여 정책

참고 계정 관리 중지가 수신될 경우 Cisco ISE에서 원래 IP 주소로 프로파일링된 엔드포인트를 다시 프로파일링합니다. 따라서 IP 주소로 프로파일링된 엔드포인트에 대한 사용자 맞춤화 프로파일이 있는 경우 이러한 프로파일의 전체 확실성 요인을 충족하는 유일한 방법은 해당 IP 주소에 일치시키는 것입니다.

네트워크 스캔(NMAP) 프로브

Cisco ISE를 사용하면 NMAP 보안 스캐너를 사용하여 서브넷에서 디바이스를 탐지할 수 있습니다. 프로파일링 서비스를 실행할 수 있는 정책 서비스 노드에서 NMAP 프로브를 활성화합니다. 엔드포인트 프로파일링 정책에서 해당 프로브의 결과를 사용합니다.

각 NMAP 수동 서브넷 스캔에는 고유한 숫자 ID가 있으며, 이는 엔드포인트 소스 정보를 해당 스캔 ID로 업데이트하는 데 사용됩니다. 엔드포인트가 탐지되면 네트워크 스캔 프로브로 검색되었음을 나타내도록 엔드포인트 소스 정보도 업데이트됩니다.

NMAP 수동 서브넷 스캔은 프린터와 같이 정적 IP 주소가 할당되어 있는 디바이스를 탐지하는 데 유용합니다. 정적 IP 주소는 Cisco ISE 네트워크에 지속적으로 연결되어 있는 디바이스에 할당되므로 이러한 디바이스는 다른 프로브에 의해 검색되지 않습니다.

NMAP 스캔 제한

서브넷을 스캔할 때는 리소스를 매우 많이 사용합니다. 서브넷 스캔은 오랫동안 진행되는 프로세스로, 시간은 서브넷의 크기와 밀도에 따라 달라집니다. 활성 스캔의 수는 항상 한 개 스캔으로 제한됩니다. 즉, 서브넷은 한 번에 하나씩만 스캔할 수 있습니다. 서브넷 스캔이 진행 중인 동안 언제든지 서브넷 스캔을 취소할 수 있습니다. **Click(**클릭**)**을 사용하여 최신 스캔 결과 링크를 표시하면 **Work Centers(**작업 센터**)** > **Profiler(**프로파일러**)** > **Manual Scans(**수동 스캔**)** > **Manual NMAP Scan Results(**수동 **NMAP** 스캔 결과**)**에 저장되어 있는 최신 네트워크 스캔 결과를 확인할 수 있습니다.

수동 **NMAP** 스캔

다음 NMAP 명령은 서브넷을 스캔하여 출력을 nmapSubnet.log로 보냅니다.

```
nmap -O -sU -p U:161,162 -oN /opt/CSCOcpm/logs/nmapSubnet.log
    --append-output -oX - <subnet>
```

표 ***45:*** 수동 서브넷 스캔용 ***NMAP*** 명령

-O	OS 탐지를 활성화합니다.
-sU	UDP를 스캔합니다.
-p <포트 범위>	지정된 포트만 스캔합니다. 예를 들면 U:161, 162와 같이 입력합니다.
oN	일반 출력을 생성합니다.
oX	XML 출력을 생성합니다.

NMAP 수동 서브넷 스캔용 SNMP 읽기 전용 커뮤니티 문자열

NMAP 수동 서브넷 스캔 결과 엔드포인트에서 UDP 포트 161이 열려 있어 속성을 더 수집할 수 있는 것으로 검색될 때마다 해당 스캔에서 SNMP 쿼리가 추가로 수행됩니다. NMAP 수동 서브넷 스캔을 수행하는 동안 네트워크 스캔 프로브는 디바이스에서 SNMP 포트 161이 열려 있는지를 탐지합니다. 포트가 열려 있으면 SNMP 버전 2c를 통해 기본 커뮤니티 문자열(public)을 사용하여 SNMP 쿼리가 트리거됩니다.

디바이스가 SNMP를 지원하며 기본 읽기 전용 커뮤니티 문자열이 public으로 설정되어 있으면 MIB 값 "ifPhysAddress"에서 디바이스의 MAC 주소를 가져올 수 있습니다.

또한 **Profiler Configuration(**프로파일러 컨피그레이션**)** 창에서 쉼표로 구분된 추가 SNMP 읽기 전용 커뮤니티 문자열을 NMAP 수동 네트워크 스캔용으로 구성할 수도 있습니다. SNMP 버전 1 및 2c를 통한 SNMP MIB walk용으로 새 읽기 전용 커뮤니티 문자열을 지정할 수도 있습니다. SNMP 읽기 전용 커뮤니티 문자열 구성에 대한 자세한 내용은 CoA, SNMP RO 커뮤니티 및 엔드포인트 속성 필터 설정, 202 페이지를 참조하십시오.

수동 NMAP 스캔 결과

최신 네트워크 스캔 결과는 Work Centers (작업 센터)> Profiler (프로파일러)> Manual Scans (수동 스캔)> Manual NMAP Scan Results (수동 NMAP 스캔 결과)에 저장됩니다. 수동 NMAP 스캔 결과 페이지에는 서브넷에서 수행하는 수동 네트워크 스캔의 결과로 탐지된 최신 엔드포인트만 표시되며, 이러한 엔드포인트에 연결된 엔드포인트 프로파일, 해당 MAC 주소 및 정적 할당 상태가 함께 표시됩니다. 필요한 경우 이 페이지에서 보다 적절한 분류를 위해 엔드포인트 서브넷에서 탐지된 포인트를 편집할 수 있습니다.

Cisco ISE에서는 프로파일링 서비스를 실행하도록 활성화된 정책 서비스 노드에서 수동 네트워크 스캔을 수행할 수 있습니다. 정책 서비스 노드에서 수동 네트워크 스캔을 실행하려면 구축의 기본 관리 ISE 노드 사용자 인터페이스에서 정책 서비스 노드를 선택해야 합니다. 서브넷에서 수동 네트워크 스캔을 수행하는 동안 네트워크 스캔 프로브는 지정한 서브넷의 엔드포인트와 해당 운영체제를 탐지하고 UDP 포트 161 및 162에서 SNMP 서비스를 확인합니다.

아래에는 수동 NMAP 스캔 결과와 관련된 추가 정보가 나와 있습니다.

- 알 수 없는 엔드포인트를 탐지하려면 NMAP에서 NMAP 또는 지원되는 SNMP 스캔을 통해 IP/MAC 바인딩을 학습할 수 있어야 합니다.
- ISE는 Radius 인증 또는 DHCP 프로파일링을 통해 알려진 엔드포인트의 IP/MAC 바인딩을 학습합니다.
- IP/MAC 바인딩은 구축의 PSN 노드간에 복제되지 않습니다. 따라서 로컬 데이터베이스에 IP / MAC 바인딩이 있는 PSN에서 수동 스캔을 트리거해야 합니다(예: MAC 주소가 마지막으로 인증 된 PSN).
- NMAP 스캔 결과에는 NMAP가 이전에 수동으로 또는 자동으로 스캔한 엔드포인트와 관련된 정보가 표시되지 않습니다.

DNS 프로브

Cisco ISE 구축에서 DNS(Domain Name Service) 프로브를 사용하면 프로파일러가 엔드포인트를 조회하고 FQDN(Fully Qualified Domain Name)을 가져올 수 있습니다. Cisco ISE 지원 네트워크에서 엔드포인트가 탐지되고 나면 엔드포인트 속성 목록이 NetFlow, DHCP, DHCP SPAN, HTTP, RADIUS 또는 SNMP 프로브에서 수집됩니다.

독립형 환경 또는 분산형 환경에서 처음으로 Cisco ISE를 구축하는 경우 설치 유틸리티를 실행하여 Cisco ISE 어플라이언스를 구성하도록 메시지가 표시됩니다. 설치 유틸리티를 실행하는 경우 DNS(Domain Name System) 도메인 및 기본 네임서버(기본 DNS 서버)를 구성합니다. 설치 중에 하나 이상의 네임서버를 구성할 수 있습니다. 나중에 CLI 명령을 사용하여 Cisco ISE를 구축한 후에는 DNS 네임서버를 변경하거나 추가할 수 있습니다.

DNS 조회 FQDN

DNS 조회를 수행하려면 DHCP, DHCP SPAN, HTTP, RADIUS 또는 SNMP 프로브 중 하나를 DNS 프로브와 함께 시작해야 합니다. 이렇게 하면 프로파일러의 DNS 프로브가 Cisco ISE 구축에 정의하는 지정된 이름 서버에 대한 역방향 DNS 조회(FQDN 조회)를 수행할 수 있습니다. 새 속성은 엔드포인트 프로파일링 정책 평가에 사용할 수 있는 엔드포인트의 속성 목록에 추가됩니다. FQDN은 시스템 IP 사전에 있는 새 속성입니다. 엔드포인트 프로파일링 조건을 생성하여 프로파일링을 위해 FQDN 속성 및 해당 값을 검증할 수 있습니다. 다음은 DNS 조회에 필요한 특정 엔드포인트 속성 및 이러한 속성을 수집하는 프로브입니다.

- dhcp-requested-address 속성 - DHCP 및 DHCP SPAN 프로브에서 수집되는 속성
- SourceIP 속성 - HTTP 프로브에서 수집되는 속성
- Framed-IP-Address 속성 - RADIUS 프로브에서 수집되는 속성
- cdpCacheAddress 속성 - SNMP 프로브에서 수집되는 속성

WLC 웹 인터페이스에서 호출 스테이션 ID 유형 구성

WLC 웹 인터페이스를 사용하여 호출 스테이션 ID 유형 정보를 구성할 수 있습니다. WLC 웹 인터페이스의 Security(보안) 탭으로 이동하여 RADIUS 인증 서버 페이지에서 호출 스테이션 ID를 구성할 수 있습니다. WLC 사용자 인터페이스에서 MAC Delimiter(MAC 구분 기호) 필드는 기본적으로 콜론으로 설정됩니다.

WLC 웹 인터페이스에서 이 정보를 구성하는 방법에 대한 자세한 내용은 Cisco Wireless LAN Controller 컨피그레이션 설명서(릴리스 7.2)에서 6장 "보안 솔루션 구성"을 참고하십시오.

config radius callStationIdType 명령을 사용하여 WLC CLI에서 이 정보를 구성하는 방법에 대한 자세한 내용은 Cisco Wireless LAN Controller 명령 참조 설명서(릴리스 7.2)에서 2장 "컨트롤러 명령"을 참고하십시오.

단계 **1** Wireless LAN Controller 사용자 인터페이스에 로그인합니다.

단계 **2** **Security(**보안**)**를 클릭합니다.

단계 **3** **AAA**를 확장하고 **RADIUS** > **Authentication(**인증**)**을 선택합니다.

단계 **4** 호출 스테이션 ID 유형 드롭다운 목록에서 **System MAC Address(**시스템 **MAC** 주소**)**를 선택합니다.
단계 **5** MAC 구분 기호 드롭다운 목록에서 **Colon(**콜론**)**을 선택합니다.

SNMP 쿼리 프로브

노드 편집 페이지에서 SNMP 쿼리 프로브를 구성해야 할 뿐 아니라 **Administration(**관리**)** > **Network Resources(**네트워크 리소스**)** > **Network Devices(**네트워크 디바이스**)** 위치에서 다른 단순 관리 프로토콜 설정도 구성해야 합니다.

네트워크 디바이스 목록 페이지에서 새 NAD(Network Access Devices)의 SNMP 설정을 구성할 수 있습니다. 네트워크 액세스 디바이스의 SNMP 설정 또는 SNMP 쿼리 프로브에서 지정하는 폴링 간격에 따라 일정한 간격으로 NAD를 쿼리합니다.

다음 컨피그레이션에 따라 특정 NAD에 대해 SNMP 쿼리를 켜고 끌 수 있습니다.

- 링크 작동 및 새 MAC 알림에서 SNMP 쿼리 켜기/끄기
- 링크 작동 및 새 MAC 알림에서 Cisco Discovery Protocol 정보에 대한 SNMP 쿼리 켜기/끄기
- 각 스위치에 대한 SNMP 쿼리 타이머(기본적으로 1시간마다)

iDevice 및 SNMP를 지원하지 않는 기타 모바일 디바이스의 경우에는 ARP 표을 통해 MAC 주소를 검색할 수 있습니다. SNMP 쿼리 프로브를 사용하여 네트워크 액세스 디바이스에서 이 표을 쿼리할 수 있습니다.

SNMP 쿼리를 사용한 Cisco Discovery Protocol 지원

네트워크 디바이스에서 SNMP 설정을 구성하는 경우 네트워크 디바이스의 모든 포트에서 Cisco Discovery Protocol이 활성화(기본값)되어 있는지 확인해야 합니다. 네트워크 디바이스의 포트에서 Cisco Discovery Protocol을 비활성화하면 연결된 일부 엔드포인트의 Cisco Discovery Protocol 정보를 놓치게 되므로 올바르게 프로파일링하지 못할 수 있습니다. 네트워크 디바이스에 대해 cdp run 명령을 사용하여 Cisco Discovery Protocol을 전역적으로 활성화하고, 네트워크 액세스 디바이스의 인터페이스에 대해 cdp enable 명령을 사용하여 Cisco Discovery Protocol을 활성화할 수 있습니다. 네트워크 디바이스 및 인터페이스에서 Cisco Discovery Protocol을 비활성화하려면 명령 시작 부분에 no keyword를 사용해 주십시오.

SNMP 쿼리를 사용한 Link Layer Discovery Protocol 지원

Cisco ISE 프로파일러는 SNMP 쿼리를 사용하여 LLDP 속성을 수집합니다. RADIUS 프로브를 사용하여 네트워크 디바이스에 내장된 Cisco IOS 센서에서 LLDP 속성을 수집할 수도 있습니다. 아래 표에서 LLDP 전역 구성을 구성하는 데 사용할 수 있는 기본 LLDP 구성 설정과, 네트워크 액세스 디바이스의 LLDP 인터페이스 구성 명령을 확인해 주십시오.

표 ***46:*** 기본 ***LLDP*** 컨피그레이션

속성	설정
LLDP global state	비활성화

속성	설정
LLDP holdtime(폐기 전)	120초
LLDP timer(패킷 업데이트 빈도)	30초
LLDP reinitialization delay	2초
LLDP tlv-select	활성화됨(모든 TLV를 보내고 받을 수 있음)
LLDP interface state	활성화됨
LLDP receive	활성화됨
LLDP transmit	활성화됨
LLDP med-tlv-select	활성화됨(모든 LLDP-MED TLV를 보낼 수 있음)

단일 문자로 표시되는 **CDP** 및 **LLDP** 기능 코드

엔드포인트의 속성 목록에는 lldpCacheCapabilities 및 lldpCapabilitiesMapSupported 속성에 대한 단일 문자 값이 표시됩니다. 이 값은 CDP 및 LLDP를 실행하는 네트워크 액세스 디바이스에 대해 표시되는 기능 코드입니다.

예 **1**

```
lldpCacheCapabilities S
lldpCapabilitiesMapSupported S
```

예 **2**

```
lldpCacheCapabilities B;T
lldpCapabilitiesMapSupported B;T
```

예 **3**

```
Switch#show cdp neighbors
Capability Codes:
R - Router, T - Trans Bridge, B - Source Route Bridge, S - Switch, H - Host, I - IGMP,
r - Repeater, P - Phone, D - Remote, C - CVTA, M - Two-port Mac Relay
...
Switch#

Switch#show lldp neighbors
Capability codes:
(R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
(W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other
...
Switch#
```

SNMP 트랩 프로브

SNMP 트랩은 MAC 알림, linkup, linkdown 및 알림을 지원하는 특정 네트워크 액세스 디바이스에서 정보를 수신합니다. SNMP 트랩 프로브는 포트가 작동하거나 작동이 중지될 때와 엔드포인트가 네트워크에 연결되거나 네트워크에서 연결이 끊길 때 특정 네트워크 액세스 디바이스에서 정보를 수신합니다.

SNMP 트랩이 완전히 작동하고 엔드포인트를 생성하도록 하려면 트랩 수신 시 SNMP 쿼리 프로브가 네트워크 액세스 디바이스의 특정 포트에서 폴링 이벤트를 트리거하도록 SNMP 쿼리를 활성화해야 합니다. 이 기능이 완전히 작동하도록 하려면 네트워크 액세스 디바이스 및 SNMP 트랩을 구성해야 합니다.

참고 Cisco ISE는 WLC(Wireless LAN Controller) 및 AP(Access Points)에서 수신된 SNMP 트랩을 지원하지 않습니다.

Active Directory 프로브

AD(Active Directory) 프로브:

- Windows 엔드포인트의 OS 정보의 신뢰도를 개선합니다. Microsoft AD는 버전 및 서비스 팩 레벨을 비롯하여 AD에 가입된 컴퓨터의 세부 OS 정보를 추적합니다. AD 프로브는 AD Runtime 커넥터를 사용하여 이 정보를 직접 검색하므로 신뢰도가 높은 클라이언트 OS 정보 소스를 제공합니다.
- 기업 자산과 그 외의 자산을 쉽게 구분할 수 있습니다. AD 프로브에서 사용할 수 있는 기본적이지만 중요한 속성은 AD에 엔드포인트가 있는지 여부입니다. 이 정보는 AD에 포함된 엔드포인트를 관리되는 디바이스 또는 기업 자산으로 분류하는 데 사용될 수 있습니다.

Administration(관리**)** > **System(**시스템**)** > **Deployment(**구축**)** > **Profiling Configuration(**프로파일링 컨피그레이션**)**에서 AD 프로브를 활성화할 수 있습니다. 이 프로브가 활성화되면 Cisco ISE는 호스트 이름을 수신하는 즉시 새 엔드포인트에 대한 AD 속성을 가져옵니다. 호스트 이름은 일반적으로 DHCP 또는 DNS 프로브에서 학습됩니다. 호스트 이름이 정상적으로 검색되면 ISE는 다시 스캔 타이머가 만료될 때까지 AD에서 같은 엔드포인트를 다시 쿼리하지 않습니다. 이는 속성 쿼리를 위한 AD의 로드를 제한하기 위한 것입니다. **Days Before Rescan(**다시 스캔할 때까지의 기간**(**일**))** 필드 (**Administration(**관리**)** > **System(**시스템**)** > **Deployment(**구축**)** > **Profiling Configuration(**프로파일링 컨피그레이션**)** > **Active Directory**)에서 다시 스캔 타이머를 구성할 수 있습니다. 엔드포인트에서 추가 프로파일링 활동이 수행되는 경우 AD를 다시 쿼리합니다.

다음 AD 프로브 속성은 ACTIVEDIRECTORY 조건을 사용하여 **Policy(**정책**)** > **Policy Elements(**정책 요소**)** > **Profiling(**프로파일링**)**에서 일치 여부를 확인할 수 있습니다. AD 프로브를 사용하여 수집한 AD 속성은 **Context Visibility(**상황 가시성**)** > **Endpoints(**엔드포인트**)** 창의 엔드포인트 세부정보에 "AD" 접두사가 붙은 채로 표시됩니다.

- AD-Host-Exists
- AD-Join-Point

- AD-Operating-System
- AD-OS-Version
- AD-Service-Pack

Cisco ISE 노드별 프로브 구성

구축에서 정책 서비스 페르소나 역할을 하는 Cisco ISE 노드별로 Profiling Configuration(프로파일링 컨피그레이션) 탭에서 하나 이상의 프로브를 구성할 수 있습니다. 여기에는 다음과 같은 노드가 포함될 수 있습니다.

- 독립형 노드: 기본적으로 관리, 모니터링 및 정책 서비스 페르소나 역할을 모두 수행하는 단일 노드에서 Cisco ISE를 구축한 경우입니다.
- 여러 노드: 구축에서 정책 서비스 페르소나 역할을 하는 노드를 둘 이상 등록한 경우입니다.

참고 모든 프로브가 기본적으로 활성화되어 있지는 않습니다. 일부 프로브는 확인 표시로 명시적으로 활성화되지 않은 경우에도 부분적으로 활성화됩니다. 프로파일링 컨피그레이션은 현재 각 PSN에 고유합니다. 구축의 각 PSN은 동일한 프로파일러 컨피그레이션 설정으로 구성하는 것이 좋습니다.

시작하기 전에

Cisco ISE 노드별 프로브는 관리 노드에서만 구성할 수 있습니다. 분산형 구축의 보조 관리 노드에서는 이 구성 기능이 제공되지 않습니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Deployment(**구축**)**를 선택합니다.

단계 **2** 정책 서비스 페르소나 역할을 하는 Cisco ISE 노드를 선택합니다.

단계 **3** 구축 노드 페이지에서 **Edit(**편집**)**를 클릭합니다.

단계 **4** **General Settings(**일반 설정**)** 탭에서 **Policy Service(**정책 서비스**)** 확인란을 선택합니다. Policy Service(정책 서비스) 확인란 선택을 취소하면 세션 서비스와 프로파일링 서비스 확인란이 모두 비활성화됩니다.

단계 **5** **Enable Profiling Services(**프로파일링 서비스 활성화**)** 확인란을 선택합니다.

단계 **6** **Profiling Configuration(**프로파일링 컨피그레이션**)** 탭을 클릭합니다.

단계 **7** 각 프로브에 대한 값을 구성합니다.

단계 **8** 프로브 컨피그레이션을 저장하려면 **Save(**저장**)**를 클릭합니다.

CoA, SNMP RO 커뮤니티 및 엔드포인트 속성 필터 설정

Cisco ISE에서는 프로파일러 컨피그레이션 페이지에서 CoA(Change of Authorization)를 실행하는 전역 컨피그레이션을 사용할 수 있습니다. 그러면 프로파일링 서비스가 이미 인증된 엔드포인트를 보다 자세하게 제어할 수 있습니다.

또한 프로파일러 컨피그레이션 페이지에서 쉼표로 구분된 추가 SNMP 읽기 전용 커뮤니티 문자열을 NMAP 수동 네트워크 스캔용으로 구성할 수도 있습니다. SNMP RO 커뮤니티 문자열은 Current custom SNMP community strings(현재 맞춤 SNMP 커뮤니티 문자열) 필드에 표시되는 것과 같은 순서로 사용됩니다.

프로파일러 컨피그레이션 페이지에서 엔드포인트 속성 필터링을 구성할 수도 있습니다.

단계 **1** **Administration(**관리**)** > **System(**시스템**)** > **Settings(**설정**)** > **Profiling(**프로파일링**)**을 선택합니다.

단계 **2** 다음 설정 중 하나를 선택하여 CoA 유형을 구성합니다.

- **No CoA(CoA** 없음**)**(기본값) - 이 옵션을 사용하여 CoA 전역 컨피그레이션을 비활성화할 수 있습니다. 이 설정은 엔드포인트 프로파일링 정책별로 구성된 CoA를 재정의합니다. 목표가 가시성에 국한되어 있다면 기본값인 **No CoA(CoA** 없음**)**를 그대로 사용하십시오.
- **Port Bounce(**포트 반송**)** - 세션이 하나뿐인 스위치 포트가 있는 경우 이 옵션을 사용할 수 있습니다. 세션이 여러 개인 포트가 있는 경우에는 Reauth(재인증) 옵션을 사용합니다. 프로파일 변경 사항에 따라 액세스 정책을 즉시 업데이트하는 것이 목표라면 **Port Bounce(**포트 바운스**)** 옵션을 선택합니다. 그러면 클라이언트리스 엔드포인트가 다시 권한 부여되고 필요한 경우 IP 주소가 새로 고쳐집니다.
- **Reauth(**재인증**)** - 이 옵션을 사용하면 이미 인증된 엔드포인트를 프로파일링할 때 재인증을 시행할 수 있습니다. 현재 세션의 재인증 후에 VLAN 또는 주소가 변경되지 않을 경우 **Reauth(**재인증**)** 옵션을 선택합니다.

  참고 단일 포트에 여러 활성 세션이 있는 경우에는 **Port Bounce(**포트 반송**)** 옵션을 사용하여 CoA를 구성했더라도 프로파일링 서비스는 **Reauth(**재인증**)** 옵션을 사용하여 CoA를 실행합니다. 이 기능을 사용하면 **Port Bounce(**포트 반송**)** 옵션 사용 시 발생할 수 있는 상황인 다른 세션의 연결 끊김을 방지할 수 있습니다.

단계 **3** **Change Custom SNMP Community Strings(**맞춤 **SNMP** 커뮤니티 문자열 변경**)** 필드에 SNMP 수동 네트워크 스캔용 새 SNMP 커뮤니티 문자열을 쉼표로 구분하여 입력하고 **Confirm Custom SNMP Community Strings(**맞춤 **SNMP** 커뮤니티 문자열 확인**)** 필드에 확인을 위해 문자열을 다시 입력합니다.

기본 커뮤니티 문자열은 공개됩니다. 이를 확인하려면 **Current Custom SNMP Community Strings(**현재 맞춤 **SNMP** 커뮤니티 문자열**)** 섹션에서 **Show(**표시**)**를 클릭합니다.

단계 **4** **Endpoint Attribute Filter(**엔드포인트 속성 필터**)** 확인란을 선택하여 엔드포인트 속성 필터링을 활성화합니다.

EndPoint Attribute Filter(엔드포인트 속성 필터**)**를 활성화하면 Cisco ISE 프로파일러는 중요한 속성만 유지하고 다른 모든 속성은 버리게 됩니다. 자세한 내용은 엔드포인트 속성 필터링을 위한 전역 설정, 206 페이지 및 ISE 데이터베이스 지속성 및 성능의 속성 필터, 205 페이지 섹션을 참조하십시오. 모범 사례로서 프로덕션 구축에서 **Endpoint Attribute Filter(**엔드포인트 속성 필터**)**를 활성화하는 것이 좋습니다.

단계 **5** Cisco ISE가 ISE에서 엔드포인트 온보딩을 분류하기 위해 이 데이터가 필요한 pxGrid 가입자에게 엔드포인트 프로브 데이터를 게시하도록 하려면 **Enable Probe Data Publisher(**프로브 데이터 게시자 활성화**)** 확인란을 선택합니다. pxGrid 가입자는 초기 구축 단계에서 대량 다운로드를 사용하여 Cisco ISE에서 엔드포인트 기록을 가져올 수 있습니다. Cisco ISE는 PAN에서 업데이트될 때마다 pxGrid 가입자에게 엔드포인트 기록을 전송합니다. 이 옵션은 기본적으로 비활성화되어 있습니다.

이 옵션을 활성화할 경우 pxGrid 페르소나가 구축에서 활성화되어 있는지 확인합니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

인증된 엔드포인트에 대한 **Change of Authorization**의 전역 컨피그레이션

전역 컨피그레이션 옵션을 사용하여 기본값인 No CoA(CoA 없음) 옵션을 통해 CoA(Change of Authorization)를 비활성화하거나, 포트 반송 및 재인증 옵션을 통해 CoA를 활성화할 수 있습니다. Cisco ISE에서 포트 반송을 구성한 경우에도 프로파일링 서비스는 "CoA 면제" 섹션에서 설명하는 기타 CoA를 계속 실행할 수 있습니다.

선택한 전역 컨피그레이션은 더 구체적인 설정이 없는 경우에만 기본 CoA 동작을 나타냅니다. 엔드포인트 프로파일링 정책별 CoA(Change of Authorization) 컨피그레이션, 239 페이지의 내용을 참조하십시오.

RADIUS 프로브 또는 모니터링 페르소나 REST API를 사용하여 엔드포인트를 인증할 수 있습니다. RADIUS 프로브를 활성화할 수 있으며, 그러면 성능이 개선됩니다. CoA를 활성화한 경우 성능 개선을 위해 Cisco ISE 애플리케이션에서 CoA 컨피그레이션과 함께 RADIUS 프로브를 활성화하는 것이 좋습니다. 그러면 프로파일링 서비스가 수집된 RADIUS 속성을 사용하여 엔드포인트에 대해 적절한 CoA를 실행할 수 있습니다.

Cisco ISE 애플리케이션에서 RADIUS 프로브를 비활성화한 경우에는 모니터링 페르소나 REST API를 사용하여 CoA를 실행할 수 있습니다. 이 경우 프로파일링 서비스가 보다 광범위한 엔드포인트를 지원할 수 있습니다. 분산형 구축에서는 모니터링 페르소나 REST API를 사용하여 CoA를 실행하려면 네트워크에 모니터링 페르소나로 지정된 Cisco ISE 노드가 하나 이상 있어야 합니다.

Cisco ISE는 분산형 구축 내 REST 쿼리의 기본 대상으로 기본 또는 보조 모니터링 노드를 임의 지정합니다. 기본 및 보조 모니터링 노드의 세션 디렉토리 정보는 동일하기 때문입니다.

Change of Authorization 실행을 위한 활용 사례

프로파일링 서비스는 다음과 같은 경우 Change of Authorization을 실행합니다.

- 엔드포인트가 삭제됨: 엔드포인트 페이지에서 엔드포인트가 삭제되었으며 네트워크에서 엔드포인트가 제거되었거나 연결이 끊긴 경우입니다.
- 예외 작업이 구성됨: 프로파일당 예외 작업을 구성하여 해당 엔드포인트에서 비정상적이거나 예기치 않은 이벤트가 발생하는 경우입니다. 이 경우 프로파일링 서비스는 CoA를 실행하여 해당하는 정적 프로파일로 엔드포인트를 이동합니다.
- 엔드포인트를 처음으로 프로파일링함: 정적으로 할당되어 있지 않은 엔드포인트를 처음으로 프로파일링하면 프로파일이 알 수 없는 프로파일에서 알려진 프로파일로 변경됩니다.

- 엔드포인트 ID 그룹이 변경됨: 권한 부여 정책에서 사용되는 엔드포인트 ID 그룹에서 엔드포인트를 추가하거나 제거하는 경우입니다.

  이 경우 프로파일링 서비스는 엔드포인트 ID 그룹이 변경될 때 CoA를 실행하며, 다음에 대해 권한 부여 정책에서 엔드포인트 ID 그룹이 사용됩니다.

  - 엔드포인트를 동적으로 프로파일링하면 해당 엔드포인트에 대해 엔드포인트 ID 그룹이 변경됩니다.
  - 동적 엔드포인트에 대해 정적 할당 플래그가 true로 설정되어 있으면 엔드포인트 ID 그룹이 변경됩니다.

- 엔드포인트 프로파일링 정책이 변경되었으며 권한 부여 정책에서 해당 정책이 사용됨: 엔드포인트 프로파일링 정책을 변경했는데 권한 부여 정책에서 사용되는 논리적 프로파일에 해당 정책이 포함되어 있는 경우입니다. 프로파일링 정책이 일치하거나, 엔드포인트가 논리적 프로파일에 연결된 엔드포인트 프로파일링 정책에 정적으로 할당되어 있으면 엔드포인트 프로파일링 정책이 변경될 수 있습니다. 두 가지 경우 모두에서 프로파일링 서비스는 엔드포인트 프로파일링 정책이 권한 부여 정책에서 사용될 때만 CoA를 실행합니다.

CoA(Change of Authorization) 발급 예외

엔드포인트 ID 그룹을 변경할 때 정적 할당이 이미 true이면 프로파일링 서비스는 CoA를 실행하지 않습니다.

Cisco ISE가 CoA를 실행하지 않는 이유는 다음과 같습니다.

- 엔드포인트의 네트워크 연결이 끊김 - 네트워크에서 연결이 끊긴 엔드포인트가 검색되는 경우입니다.
- 인증된 유선 EAP(Extensible Authentication Protocol) 가능 엔드포인트 - 인증된 유선 EAP 가능 엔드포인트가 검색되는 경우입니다.
- 포트당 활성 세션이 여러 개임 - 단일 포트의 활성 세션이 여러 개인 경우에는 Port Bounce(포트 바운스) 옵션을 사용하여 CoA를 구성했더라도 프로파일링 서비스는 Reauth 옵션을 사용하여 CoA를 실행합니다.
- 무선 엔드포인트 탐지 시 연결 끊김 패킷 CoA(세션 종료) - 무선 엔드포인트가 검색되면 포트 반송 CoA가 아닌 연결 끊김 패킷 CoA(세션 종료)가 실행됩니다. 이처럼 CoA가 변경되므로 WLC(Wireless LAN Controller) CoA가 지원된다는 이점이 있습니다.
- 프로파일러 CoA는 Authorization Profile(권한 부여 프로파일)에서 구성된 논리적 프로파일에 대해 **Suppress Profiler CoA for endpoints in Logical Profile(**논리적 프로파일에서 엔드포인트에 대해 프로파일러 **CoA** 표시 안 함**)** 옵션을 사용하는 경우 표시되지 않습니다. 프로파일러 CoA는 기본적으로 다른 모든 엔드포인트에 대해 트리거됩니다.
- 전역 CoA 없음 설정이 정책 CoA를 재정의함 - 전역 CoA 없음은 엔드포인트 프로파일링 정책의 모든 컨피그레이션 설정을 재정의합니다. 엔드포인트 프로파일링 정책별로 구성된 CoA에 관계없이 Cisco ISE에서는 CoA가 실행되지 않기 때문입니다.

참고 이 경우 CoA 없음 및 Reauth CoA 컨피그레이션은 영향을 받지 않으며 프로파일러 서비스는 유선 엔드포인트와 무선 엔드포인트에 대해 동일한 CoA 컨피그레이션을 적용합니다.

각 **CoA** 컨피그레이션 유형에 맞게 발급되는 **CoA(Change of Authorization)**

표 ***47:*** 각 ***CoA*** 컨피그레이션 유형에 맞게 발급되는 ***CoA(Change of Authorization)***

시나리오	**No CoA(CoA** 없음**)** 컨피그레이션	**Port Bounce(**포트 바운스**)** 컨피그레이션	**Reauth(**재인증**)** 컨피그레이션	추가 정보
Cisco ISE의 전역 CoA 컨피그레이션(일반 컨피그레이션)	CoA 없음	포트 바운스	Reauthentication(재인증)	—
네트워크에서 엔드포인트 연결이 끊어짐	No CoA(CoA 없음)	No CoA(CoA 없음)	No CoA(CoA 없음)	CoA(Change of Authorization)는 RADIUS 속성 Acct-Status -Type 값 Stop으로 확인됩니다.
동일한 스위치 포트에 여러 활성 세션이 있는 무선 엔드포인트	No CoA(CoA 없음)	Reauthentication(재인증)	Reauthentication(재인증)	재인증으로 다른 세션의 연결이 끊어지지 않도록 합니다.
무선 엔드포인트	No CoA(CoA 없음)	연결 끊김 패킷 CoA(세션 종료)	Reauthentication(재인증)	Wireless LAN Controller 지원
불완전 CoA 데이터	No CoA(CoA 없음)	No CoA(CoA 없음)	No CoA(CoA 없음)	RADIUS 속성 누락으로 인해

ISE 데이터베이스 지속성 및 성능의 속성 필터

Cisco ISE는 성능 저하 문제를 해결하는 NetFlow 프로브를 제외한 Dynamic Host Configuration Protocol(DHCP 헬퍼와 DHCP SPAN 모두), HTTP, RADIUS 및 Simple Network Management Protocol 프로브용 필터를 구현합니다. 각 프로브 필터는 엔드포인트 프로파일링과 무관한 임시적 속성 목록을 포함하며 프로브에서 수집된 속성에서 그러한 속성을 제거합니다.

isebootstrap 로그(isebootstrap-yyyymmdd-xxxxxx.log)는 사전 생성 및 사전에서의 속성 필터링을 처리하는 메시지를 포함합니다. 또한 엔드포인트에서 필터링 단계를 진행하여 필터링이 발생했음을 나타내는 경우 디버깅 메시지를 기록하도록 구성할 수 있습니다.

Cisco ISE 프로파일러는 다음과 같은 엔드포인트 속성 필터를 호출합니다.

- DHCP 헬퍼와 DHCP SPAN 모두에 사용되는 DHCP 필터는 필요한 속성이 아니어서 DHCP 패킷을 구문 분석한 후 제거되는 모든 속성을 포함합니다. 필터링된 속성은 엔드포인트의 엔드포인트 캐시에 있는 기존 속성과 병합됩니다.
- HTTP 필터는 필터링 후에도 속성 집합에 커다란 변화가 없는 HTTP 패킷에서 속성을 필터링하는 데 사용됩니다.
- RADIUS 필터는 시스템 로그 구문 분석이 완료되고 엔드포인트 속성이 프로파일링 용도로 엔드포인트 캐시에 병합된 경우에 사용됩니다.
- SNMP 쿼리용 SNMP 필터는 모두 SNMP-Query 프로브에 사용되는 별도의 CDP 및 LLDP 필터를 포함합니다.

엔드포인트 속성 필터링을 위한 전역 설정

수집 지점에서 자주 변경되지 않는 엔드포인트 속성 수를 줄여 지속성 이벤트 및 복제 이벤트 수를 줄일 수 있습니다. **EndPoint Attribute Filter(**엔드포인트 속성 필터**)**를 활성화하면 Cisco ISE 프로파일러는 중요한 속성만 유지하고 다른 모든 속성은 버리게 됩니다. 중요한 속성이란 Cisco ISE 시스템에 사용되는 속성 또는 특히 엔드포인트 프로파일링 정책 또는 규칙에 사용되는 속성을 말합니다.

Endpoint Attribute Filter(엔드포인트 속성 필터**)**를 활성화하려면 CoA, SNMP RO 커뮤니티 및 엔드포인트 속성 필터 설정, 202 페이지 섹션을 참고하십시오.

허용 목록은 엔드포인트 프로파일링을 위한 사용자 맞춤화 엔드포인트 프로파일링 정책에 사용되는 일련의 속성 및 CoA(Change of Authorization), BYOD(Bring Your Own Device), DRW(Device Registration WebAuth) 등이 Cisco ISE에서 정상적으로 작동하기 위해 반드시 필요한 속성 집합입니다. 허용 목록은 엔드포인트의 소유권이 변경(여러 정책 서비스 노드에서 속성이 수집될 때)되는 경우에 항상 조건으로 사용되며, 비활성화된 경우에도 마찬가지입니다.

기본적으로 허용 목록은 비활성화되어 있으며 속성은 속성 필터가 활성화된 경우에만 삭제됩니다. 허용 목록은 프로파일링 정책에 새 속성을 포함시키는 피드를 비롯하여 엔드포인트 프로파일링 정책이 변경되면 동적으로 업데이트됩니다. 허용 목록에 없는 속성은 수집 시 즉시 삭제되며 그러한 속성은 엔드포인트 프로파일링에 사용되지 않습니다. 버퍼링과 함께 사용되는 경우 지속성 이벤트의 수는 감소할 수 있습니다.

다음 두 소스에서 확인된 속성 집합이 허용 목록에 포함되어 있는지 확인해야 합니다.

- 엔드포인트를 프로파일과 일치시킬 수 있도록 기본 프로파일에 사용되는 속성 집합
- CoA(Change of Authorization), BYOD(Bring Your Own Device), DRW(Device Registration WebAuth) 등이 정상적으로 작동하기 위해 반드시 필요한 속성 집합

참고 허용 목록에 새 속성을 추가하려면 관리자가 해당 속성을 사용하는 새 프로파일러 조건 및 정책을 생성해야 합니다. 이 새 속성은 저장 및 복제된 속성의 허용 목록에 자동으로 추가됩니다.

표 ***48:*** 허용 속성

AAA-Server	BYODRegistration
Calling-Station-ID	인증서 만료 날짜
인증서 발급 날짜	인증서 발급자 이름
인증서 일련 번호	설명
DestinationIPAddress	디바이스 식별자
디바이스 이름	DeviceRegistrationStatus
EndPointPolicy	EndPointPolicyID
EndPointProfilerServer	EndPointSource
FQDN	FirstCollection
Framed-IP-Address	IdentityGroup
IdentityGroupID	IdentityStoreGUID
IdentityStoreName	L4_DST_PORT
LastNmapScanTime	MACAddress
MatchedPolicy	MatchedPolicyID
NADAddress	NAS-IP-Address
NAS-Port-Id	NAS-Port-Type
NmapScanCount	NmapSubnetScanID
OS 버전	OUI
PolicyVersion	PortalUser
PostureApplicable	제품
RegistrationTimeStamp	—
StaticAssignment	StaticGroupAssignment
TimeToProfile	Total Certainty Factor
User-Agent	cdpCacheAddress

cdpCacheCapabilities	cdpCacheDeviceId
cdpCachePlatform	cdpCacheVersion
ciaddr	dhcp-class-identifier
dhcp-requested-address	host-name
hrDeviceDescr	ifIndex
ip	lldpCacheCapabilities
lldpCapabilitiesMapSupported	lldpSystemDescription
operating-system	sysDescr
161-udp	—

IOS 센서 내장 스위치에서의 속성 수집

IOS 센서 통합을 통해 Cisco ISE 런타임 및 Cisco ISE 프로파일러에서 스위치로부터 전송된 속성의 일부 또는 전부를 수집할 수 있습니다. RADIUS 프로토콜을 사용하여 스위치에서 직접 DHCP, CDP 및 LLDP 속성을 수집할 수 있습니다. DHCP, CDP 및 LLDP에 대해 수집된 속성은 구문 분석되고 **Policy(**정책**)** > **Policy Elements(**정책 요소**)** > **Dictionary(**사전**)** 위치에서 프로파일러 사전의 속성에 매핑됩니다.

디바이스 센서에서 지원되는 Catalyst 플랫폼에 대한 자세한 내용은 https://communities.cisco.com/docs/DOC-72932를 참고하십시오.

IOS 센서 내장 네트워크 액세스 디바이스

IOS 센서 내장 네트워크 액세스 디바이스를 Cisco ISE와 통합하면 다음 구성 요소가 통합됩니다.

- IOS 센서
- DHCP, CDP 및 LODP 데이터 수집을 위해 네트워크 액세스 디바이스(스위치)에 내장되어 있는 데이터 컬렉터
- 데이터를 처리하고 엔드포인트의 디바이스 유형을 확인하기 위한 분석기

  분석기는 두 가지 방식으로 구축할 수 있지만 이 두 방식을 함께 사용할 수는 없습니다.

  - Cisco ISE에서 분석기를 구축할 수 있습니다.
  - 스위치에 센서로 분석기를 내장할 수 있습니다.

IOS 센서 지원 네트워크 액세스 디바이스의 컨피그레이션 체크리스트

이 섹션에는 스위치로부터 직접 DHCP, CDP 및 LLDP 속성을 수집하도록 IOS 센서 지원 스위치 및 Cisco ISE에서 구성해야 하는 작업 목록이 요약되어 있습니다.

- Cisco ISE에서 RADIUS 프로브가 활성화되어 있는지 확인합니다.
- 네트워크 액세스 디바이스가 DHCP, CDP 및 LLDP 정보 수집용 IOS 센서를 지원하는지 확인합니다.
- 네트워크 액세스 디바이스가 다음 CDP 및 LLDP 명령을 실행하여 엔드포인트에서 CDP 및 LLDP 정보를 캡처하는지 확인합니다.

```
cdp enable
lldp run
```

- 세션 계정 관리가 표준 AAA 및 RADIUS 명령을 사용해 개별적으로 활성화되어 있는지 확인합니다.

  예를 들어 다음 명령을 사용합니다.

```
aaa new-model
aaa accounting dot1x default start-stop group radius

radius-server host <ip> auth-port <port> acct-port <port> key <shared-secret>
radius-server vsa send accounting
```

- IOS 센서별 명령을 실행해야 합니다.
  - 계정 관리 확대 활성화

    IOS 센서 프로토콜 데이터를 RADIUS 계정 관리 메시지에 추가하고 새 센서 프로토콜 데이터를 탐지할 때 추가적인 계정 관리 이벤트를 생성하려면 네트워크 액세스 디바이스를 활성화해야 합니다. 즉, RADIUS 계정 관리 메시지에 모든 CDP, LLDP 및 DHCP 속성이 포함되어야 합니다.

    다음 전역 명령을 입력합니다.

    device-sensor accounting

  - 계정 관리 확대 비활성화

    (계정 관리) 네트워크 액세스 디바이스를 비활성화하고 지정된 포트에서 호스팅되는 세션에 대한 IOS 센서 프로토콜 데이터를 RADIUS 계정 관리 메시지에 추가하려면(계정 관리 기능이 전역적으로 활성화된 경우) 적절한 포트에 대해 다음 명령을 입력합니다.

    no device-sensor accounting

  - TLV 변경 추적

    기본적으로 지원되는 각 피어 프로토콜의 경우, 지정된 세션 상황에서 이전에 수신하지 않은 TLV(Type, Length, Value)가 인커밍 패킷에 포함되어 있는 경우에만 클라이언트 알림 및 계정 관리 이벤트가 생성됩니다.

새 TLV가 있거나 이전에 수신한 TLV의 값이 서로 다른 모든 TLV 변경 사항에 대해 클라이언트 알림 및 계정 관리 이벤트를 활성화해야 합니다. 다음의 명령을 입력합니다.

device-sensor notify all-changes

- 네트워크 액세스 디바이스에서 IOS Device Classifier(로컬 분석기)를 비활성화해야 합니다.

  다음의 명령을 입력합니다.

```
no macro auto monitor
```

참고 이 명령은 네트워크 액세스 디바이스에서 변경당 두 개의 동일한 RADIUS 계정 관리 메시지가 전송되는 것을 차단합니다.

ISE 프로파일러를 통한 Cisco IND 컨트롤러 지원

Cisco ISE는 Cisco IND(Industrial Network Device)에 연결된 디바이스의 상태를 프로파일링하고 표시할 수 있습니다. PxGrid는 Cisco ISE와 Cisco Industrial Network Director를 연결하여 엔드포인트(IoT) 데이터와 통신합니다. Cisco ISE의 pxGrid는 Cisco IND 이벤트를 사용하고 Cisco IND를 쿼리하여 엔드포인트 유형을 업데이트합니다.

Cisco ISE 프로파일러에는 사물 인터넷(IoT) 디바이스에 대한 사전 속성이 있습니다. **Policy(**정책**)** > **Policy Elements(**정책 요소**)** > **Dictionaries(**사전**)**를 선택하고 시스템 사전 목록에서 *IOTASSET*를 선택하여 사전 속성을 확인합니다.

지침 및 권장 사항

프로파일링을 위해 여러 ISE 노드를 구성한 경우 한 노드에서만 Cisco IND에 대해 pxGrid를 활성화하는 것이 좋습니다.

여러 Cisco IND 디바이스를 단일 ISE에 연결할 수 있습니다.

둘 이상의 게시자(Cisco IND)에서 동일한 엔드포인트가 수신되는 경우 Cisco ISE는 해당 엔드포인트에 대한 마지막 게시자의 데이터만 유지합니다.

Cisco ISE는 pxGrid의 서비스 이름 *com.cisco.endpoint.asset* 및 */topic/com.cisco.endpoint.asset*에서 Cisco IND 데이터를 가져옵니다.

Cisco IND 프로파일링 프로세스 플로우

Cisco IND 에셋 검색은 IoT 디바이스를 찾고 해당 디바이스의 엔드포인트 데이터를 pxGrid에 게시합니다. Cisco ISE는 pxGrid에서 이벤트를 확인하고 엔드포인트 데이터를 가져옵니다. Cisco ISE의 프로파일러 정책은 디바이스 데이터를 ISE 프로파일러 사전의 속성에 할당하고 해당 속성을 Cisco ISE의 엔드포인트에 적용합니다.

Cisco ISE의 기존 속성을 충족하지 않는 IoT 엔드포인트 데이터는 저장되지 않습니다. 그러나 Cisco ISE에서 더 많은 속성을 생성하여 Cisco IND에 등록할 수 있습니다.

Cisco ISE는 pxGrid를 통해 Cisco IND에 대한 연결이 처음 설정될 때 엔드포인트를 대량으로 다운로드합니다. 네트워크 장애가 발생할 경우 Cisco ISE는 누적된 엔드포인트 변경 사항을 다시 한 번 대량으로 다운로드합니다.

IND 프로파일링을 위한 Cisco ISE 및 Cisco IND 구성

참고 Cisco IND에서 pxGrid를 활성화하기 전에 Cisco IND에 Cisco ISE 인증서를 설치하고 ISE에 Cisco IND 인증서를 설치해야 합니다.

1. **Administration(**관리**)** > **Deployment(**구축**)**를 선택합니다. pxGrid 사용자로 사용할 PSN을 편집하고 pxGrid를 활성화합니다. 이 PSN은 Cisco IND 및 프로파일링에서 게시한 pxGrid 데이터에서 엔드포인트를 생성합니다.
2. **Administration(**관리**)** > **pxGrid Services(pxGrid** 서비스**)**를 선택하여 pxGrid가 실행 중인지 확인합니다. 그런 다음 **Certificates(**인증서**)** 탭을 클릭하고 인증서 필드에 내용을 입력합니다. **Create(**생성**)**를 클릭하여 인증서를 발급하고 인증서를 다운로드합니다.
   - **I want to(**원하는 옵션**)**에서 **Generate a single certificate without a certificate signing request(**인증서 서명 요청 없이 단일 인증서 생성**), CN(Common Name)**을 선택하고 연결하는 Cisco IND의 이름을 입력합니다.
   - **Certificate Download Format(**인증서 다운로드 형식**)**에서 **PKS12 format(PKS12** 형식**)**을 선택합니다.
   - **Certificate Password(**인증서 비밀번호**)**에서 비밀번호를 생성합니다.

참고 ISE 내부 CA를 활성화해야 합니다. 브라우저에서 팝업을 차단한 경우 인증서를 다운로드할 수 없습니다. 다음 단계에서 PEM 파일을 사용할 수 있도록 인증서의 압축을 풉니다.

3. Cisco IND에서 **Settings(**설정**)** > **pxGrid**를 선택하고 **Download .pem IND certificate(.pem IND** 인증서 다운로드**)** 를 클릭합니다. 이 창을 열어 둡니다.
4. Cisco ISE에서 **Administration(**관리**)** > **pxGrid Services(pxGrid** 서비스**)** > **All Clients(**모든 클라이언트**)**를 선택합니다. Cisco IND pxGrid 클라이언트가 표시되면 승인합니다.
5. Cisco IND에서 슬라이더를 이동하여 pxGrid를 활성화합니다. 다른 화면이 열리면 ISE 노드의 위치, ISE에서 이 pxGrid 서버에 대해 입력한 인증서의 이름 및 입력한 비밀번호를 지정합니다. **Upload Certificate(**인증서 업로드**)**를 클릭하고 ISE pxGrid PEM 파일을 찾습니다.
6. ISE에서 **Administration(**관리**)** > **Certificates(**인증서**)** > **Trusted Certificates(**신뢰할 수 있는 인증서**)**를 선택합니다. **Import(**가져오기**)**를 클릭하고 Cisco IND에서 가져온 인증서의 경로를 입력합니다.
7. Cisco IND에서 **Activate(**활성화**)**를 클릭합니다.

8. Cisco ISE에서 **Administation(**관리**)> Deployment(**구축**)**를 선택합니다. Cisco IND 연결에 사용 중인 PSN을 선택하고 Profiling(프로파일 링) 창을 선택한 다음 pxGrid 프로브를 활성화합니다.
9. 이제 ISE와 Cisco IND 간의 pxGrid 연결이 활성화됩니다. Cisco IND에서 찾은 IoT 엔드포인트를 표시하여 확인합니다.

IND 프로파일링을 위한 속성 추가

Cisco IND는 ISE 사전에 없는 속성을 반환할 수 있습니다. Cisco ISE에 속성을 더 추가하여 해당 IoT 디바이스를 더욱 정확하게 프로파일링할 수 있습니다. 새 속성을 추가하려면 Cisco ISE에서 사용자 맞춤화 속성을 생성하고 해당 속성을 pxGrid를 통해 Cisco IND로 전송합니다.

1. **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **Settings(**설정**)**를 선택한 다음 **Endpoint Custom Attributes(**엔드포인트 사용자 맞춤화 속성**)**를 선택합니다. 속성 엔드포인트 속성을 생성합니다.
2. 이제 프로파일러 정책에서 이 속성을 사용하여 새 속성으로 에셋을 식별할 수 있습니다. **Policy(**정책**)** > **Profiling(**프로파일링**)**을 선택하고 새 프로파일러 정책을 생성합니다. **Rules(**규칙**)** 섹션에서 새 규칙을 생성합니다. 속성/값을 추가할 때 **CUSTOMATTRIBUTE** 폴더 및 생성한 사용자 맞춤화 속성을 선택합니다.

MUD에 대한 ISE 지원

제조업체 사용 설명자(MUD)는 온보드(on-board) IoT 디바이스에 대한 방법을 정의하는 IETF 표준입니다. 이는 사물 인터넷 디바이스에 대한 완벽한 가시성 및 세그멘테이션 자동화를 제공합니다. MUD는 IETF 프로세스에서 승인되었으며 RFC8520으로 릴리스되었습니다. 자세한 내용은 https://datatracker.ietf.org/doc/draft-ietf-opsawg-mud/를 참조하십시오.

Cisco ISE, 릴리스 2.6 이상에서는 IoT 디바이스 식별을 지원합니다. Cisco ISE는 프로파일링 정책 및 엔드포인트 ID 그룹을 자동으로 생성합니다. MUD는 IoT 디바이스 프로파일링, 동적으로 프로파일링 정책을 생성, 정책 및 엔드포인트 ID 그룹을 생성하는 전체 프로세스 자동화를 지원합니다. 관리자는 이러한 프로파일링 정책을 사용하여 권한 부여 정책 및 프로파일을 수동으로 생성할 수 있습니다. DHCP 및 LLDP 패킷으로 MUD URL을 전송하는 사물 인터넷 디바이스는 이러한 프로파일과 정책을 사용하여 온보딩됩니다.

Cisco ISE는 사물 인터넷 디바이스의 서명되지 않은 분류를 수행합니다. Cisco ISE는 MUD 속성을 저장하지 않습니다. 속성은 현재 세션에서만 사용됩니다. **Context and Visibility(**상황 및 가시성**)** > **Endpoints (**엔드포인트**)** 창에서 **Endpoint Profile(**엔드포인트 프로파일**)** 필드로 사물 인터넷 디바이스를 필터링할 수 있습니다.

다음 디바이스는 Cisco ISE로 MUD 데이터 전송을 지원합니다.

- Cisco Catalyst 3850 Series Switches running Cisco IOS XE Version 16.9.1 & 16.9.2
- Cisco Catalyst Digital Building Series Switches running Cisco IOS Version 15.2(6)E2
- Cisco Industrial Ethernet 4000 Series Switches running Cisco IOS Version 15.2(6)E2
- MUD 기능이 내장된 사물 인터넷(IoT) 디바이스

Cisco ISE는 다음 프로파일링 프로토콜 및 프로파일링 프로브를 지원합니다.

- LLDP 및 Radius-TLV 127
- DHCP-옵션 161

두 필드 모두 IOS Device Sensor에서 Cisco ISE로 전송할 수 있습니다.

MUD를위한 ISE 구성

1. **Work Centers(**작업 센터**)** > **Profiler(**프로파일러**)** > **Profiler Settings(**프로파일러 설정**)**를 선택하고 **Enable profiling for MUD (MUD**용 프로파일링 활성화**)** 확인란을 선택합니다.
2. ISE에 MUD URI를 보낼 수 있는 네트워크 액세스 디바이스 추가 네트워크 디바이스를 추가하려면 **Administration(**관리**)** > **Network Resources(**네트워크 리소스**)** > **Network Devices(**네트워크 디바이스**)**를 선택합니다.
3. MUD-URL 연결이 작동하는지 확인합니다.
    1. **Context Visibility(**상황 가시성**)** > **Endpoints(** 엔드포인트**)**를 선택하고 ISE가 성공적으로 분류한 사물 인터넷 엔드포인트를 찾습니다. **IOT-MUD**로 시작하는 엔드포인트 프로파일 이름으로 사물 인터넷 디바이스를 필터링할 수 있습니다.
    2. 사물 인터넷 디바이스 중 한 개 디바이스의 엔드포인트 MAC 주소를 클릭하고 속성 태그를 선택합니다. 속성 목록에 mud-url이 있는지 확인합니다.
    3. **Policy(**정책**)** > **Profiling(**프로파일링**)**을 선택하고 **System Type(**시스템 유형**)**으로 **IOT Created(IOT** 생성됨**)**를 선택하여 목록을 필터링합니다.
4. 필요에 따라 새 사물 인터넷 디바이스에 대한 디버그 로깅을 구성합니다.
    1. System Logging Debug Log Configuration (시스템 로깅 디버그 로그 컨피그레이션)을 선택하고 MUD 컨피그레이션이있는 ISE 노드를 선택합니다. > >
    2. 왼쪽 메뉴에서 **Debug Log Configuration(**디버그 로그 컨피그레이션**)**을 선택한 다음 프로파일러를 선택합니다.

더 많은 사물 인터넷 디바이스가 분류됨에 따라 동일한 카테고리 또는 동일한 MUD-URL 을 갖는 동일한 그룹의 모든 디바이스가 동일한 엔드포인트 그룹으로 할당됩니다. 예를 들어, Molex 라이트가 연결되고 분류된 경우 해당 Molex 라이트에 대한 프로파일러 그룹이 생성됩니다. 동일한 유형(MUD-URL이 동일한)의 더 많은 Molex 라이트가 분류됨에 따라 동일한 분류 또는 엔드포인트 ID 그룹을 상속합니다.

ISE 및 Switch에서 MUD 트래픽 흐름 확인

1. 사물 인터넷 디바이스를 켜기 전에 포트를 연결하거나 인터페이스를 활성화합니다.
    1. ISE에서 패킷 캡처를 시작합니다.
    2. 스위치 포트에서 패킷 캡처를 시작합니다.

2. 스위치에서 다음 출력을 확인합니다.
    1. **show device-sensor cache all**
    2. **show access-session**
    3. **show radius statistics**
3. 사물 인터넷 디바이스를 켭니다.
4. 1분마다 다음을 반복합니다.
    1. **show device-sensor cache all**
    2. **show access-session**
    3. **show radius statistics**
5. 모든 디바이스가 ISE에 표시될 때까지 3 ~ 5분 동안 기다립니다.
6. ISE 및 스위치 패킷 캡쳐를 중단합니다.
7. 1분마다 다음을 반복합니다.
    1. **show device-sensor cache all**
    2. **show access-session**
    3. **show radius statistics**

프로파일러 조건

프로파일링 조건은 다른 조건과 유사한 정책 요소입니다. 그러나 인증, 권한 부여 및 게스트 조건과 달리 프로파일링 조건은 제한된 수의 속성을 기반으로 할 수 있습니다. 프로파일러 조건 페이지에는 Cisco ISE에서 사용 가능한 속성과 해당 설명이 나열됩니다.

프로파일러 조건은 다음 중 하나일 수 있습니다.

- Cisco 제공: Cisco ISE는 구축될 때 미리 정의된 프로파일링 조건을 포함하는데, 그러한 조건은 프로파일러 조건 페이지에서 Cisco 제공으로 식별됩니다. Cisco 제공 프로파일링 조건은 삭제할 수 없습니다.

  Policy(정책**) > Policy Elements(**정책 요소**) > Dictionaries(**사전**) > System(**시스템**)** 위치에 있는 시스템 프로파일러 사전에서도 Cisco 제공 조건을 찾을 수 있습니다.

  MAC 사전을 예를 들 수 있습니다. 일부 제품에서 OUI(Organizationally Unique Identifier)는 디바이스 구성을 식별하고 만들 때 우선적으로 사용하는 고유한 속성입니다. 디바이스 MAC 주소의 구성 요소인 MAC 사전에는 MACAddress 및 OUI 속성이 있습니다.

- 관리자 생성: Cisco ISE 관리자가 생성하는 프로파일러 조건 또는 복제되어 미리 정의된 프로파일링 조건은 관리자 생성으로 식별됩니다. 프로파일러 조건 창에서 프로파일러 사전을 사용하

여 DHCP, MAC, SNMP, IP, RADIUS, NetFlow, CDP, LLDP 및 NMAP 유형의 프로파일러 조건을 생성할 수 있습니다.

프로파일링 정책 수의 권장 상한은 1,000개이지만 프로파일링 정책은 최대 2,000개까지 늘릴 수 있습니다.

네트워크 스캔 작업 프로파일링

엔드포인트 스캔 작업은 엔드포인트 프로파일링 정책에서 참조될 수 있으며 네트워크 스캔 작업과 연결된 조건이 충족되는 경우 트리거되는 구성 가능한 작업입니다.

엔드포인트 스캔은 Cisco ISE 시스템에서 리소스 사용량을 제한하기 위해 엔드포인트를 스캔하는 데 사용됩니다. 네트워크 스캔 작업은 리소스를 많이 사용하는 네트워크 스캔과 달리 단일 엔드포인트를 스캔합니다. 그에 따라 전반적인 엔드포인트 분류 기능이 개선돼 엔드포인트에 대한 엔드포인트 프로파일이 수정됩니다. 엔드포인트 스캔은 한 번에 하나씩만 처리될 수 있습니다.

단일 네트워크 스캔 작업을 엔드포인트 프로파일링 정책에 연결할 수 있습니다. Cisco ISE에는 네트워크 스캔 작업에 대한 3가지 스캔 유형이 미리 정의되어 있습니다. 3가지 스캔 유형(예: OS-scan, SNMPPortsAndOS-scan 및 CommonPortsAndOS-scan)이 모두 포함되거나 하나만 포함될 수 있습니다. Cisco ISE에서 미리 정의된 네트워크 스캔 작업인 OS-scan, SNMPPortsAndOS-scan 및 CommonPortsAndOS-scans는 편집하거나 삭제할 수 없습니다. 고유한 네트워크 스캔 작업을 새로 생성할 수도 있습니다.

엔드포인트가 적절히 프로파일링된 경우 해당 엔드포인트에 대해 구성한 네트워크 스캔 작업을 사용할 수 없습니다. 예를 들어 Apple-Device를 스캔하면 스캔된 엔드포인트를 Apple 디바이스로 분류할 수 있습니다. OS-scan에 따라 엔드포인트가 실행되고 있는 운영체제가 확인되면 Apple-Device 프로파일에 더 이상 일치되지 않으며 Apple 디바이스에 대한 적절한 프로파일에 일치됩니다.

네트워크 스캔 작업 생성

엔드포인트 프로파일링 정책과 연결되어 있는 네트워크 스캔 작업에서는 엔드포인트에서 운영체제, SNMP(Simple Network Management Protocol) 포트 및 일반 포트를 스캔합니다. Cisco에서는 가장 일반적인 NMAP 스캔을 위한 네트워크 스캔 작업을 제공하지만 원하는 작업을 생성할 수도 있습니다.

새 네트워크 스캔을 생성할 때는 NMAP 프로브가 스캔하도록 할 정보의 유형을 정의합니다.

시작하기 전에

네트워크 스캔(NMAP) 프로브를 활성화해야 네트워크 스캔 작업을 트리거하는 규칙을 정의할 수 있습니다. 해당 절차는 Cisco ISE 노드별 프로브 구성에 설명되어 있습니다.

단계 **1** **Policy**(정책) > **Policy Elements**(정책 요소) > **Results**(결과) > **Profiling**(프로파일링) > **Network Scan (NMAP) Actions**(네트워크 스캔(**NMAP**) 작업)를 선택합니다. **Work Centers**(작업 센터) > **Profiler**(프로파일러) > **Policy Elements**(정책 요소) > **NMAP Scan Actions**(**NMAP** 스캔 작업).

단계 **2** **Add**(추가)를 클릭합니다.

단계 **3** 생성할 네트워크 스캔 작업의 이름과 설명을 입력합니다.

단계 **4** 엔드포인트에서 다음을 스캔하려는 경우 하나 이상의 확인란을 선택합니다.

- Scan OS(OS 스캔): 운영체제를 스캔하려는 경우 선택합니다.
- Scan SNMP Port(SNMP 포트 스캔): SNMP 포트(161, 162)를 스캔하려는 경우 선택합니다.
- Scan Common Port(일반 포트 스캔): 일반 포트를 스캔하려는 경우 선택합니다.
- Scan Custom Ports(맞춤형 포트 스캔): 맞춤형 포트를 스캔하려는 경우 선택합니다.
- Scan Include Service Version Information(스캔에 서비스 버전 정보 포함): 디바이스의 세부 설명을 포함할 수 있는 버전 정보를 스캔하려는 경우 선택합니다.
- Run SMB Discovery Script(SMB 검색 스크립트 실행): OS 및 컴퓨터 이름과 같은 정보를 검색하기 위해 SMB 포트(445 및 139)를 스캔하려는 경우 선택합니다.
- Skip NMAP Host Discovery(NMAP 호스트 검색 건너뛰기): NMAP 스캔의 초기 호스트 검색 단계를 건너뛰려는 경우 선택합니다.

  참고 Skip NMAP Host Discovery(NMAP 호스트 검색 건너뛰기) 옵션은 자동 NMAP 스캔의 경우 기본적으로 선택되지만 수동 NMAP 스캔을 실행하려면 이 옵션을 선택해야 합니다.

단계 **5** **Submit(**제출**)**을 클릭합니다.

NMAP 운영체제 스캔

OS-scan(Operating System scan) 유형에서는 엔드포인트가 실행되고 있는 운영체제(및 OS 버전)를 스캔합니다. 이 스캔에서는 리소스를 많이 사용합니다.

NMAP 툴은 OS-scan에 제한이 있어 신뢰성이 낮은 결과가 생성될 수 있습니다. 예를 들어 스위치 및 라우터와 같은 네트워크 디바이스의 운영체제를 스캔할 때 NMAP OS-scan에서 해당 디바이스에 대해 잘못된 operating-system 속성을 제공할 수 있습니다. 정확도가 100%는 아니더라도 Cisco ISE에는 operating-system 속성이 표시됩니다.

규칙에서 NMAP operating-system 속성을 사용하는 엔드포인트 프로파일링 정책이 낮은 확실성 값 조건(확실성 요인 값)을 포함하도록 구성해야 합니다. NMAP:operating-system 속성을 기반으로 하여 엔드포인트 프로파일링 정책을 생성할 때마다 NMAP에서 잘못된 결과를 필터링할 수 있도록 AND 조건을 포함하는 것이 좋습니다.

다음 NMAP 명령은 스캔 OS를 엔드포인트 프로파일링 정책과 연결할 때 운영체제를 스캔합니다.

```
nmap -sS -O -F -oN /opt/CSCOcpm/logs/nmap.log -append-output -oX - <IP-address>
```

다음 NMAP 명령은 서브넷을 스캔하여 출력을 nmapSubnet.log로 보냅니다.

```
nmap -O -sU -p U:161,162 -oN /opt/CSCOcpm/logs/nmapSubnet.log
    --append-output -oX - <subnet>
```

표 ***49:*** 수동 서브넷 스캔용 ***NMAP*** 명령

-O	OS 탐지를 활성화합니다.

-sU	UDP를 스캔합니다.
-p <포트 범위>	지정된 포트만 스캔합니다. 예를 들면 U:161, 162와 같이 입력합니다.
oN	일반 출력을 생성합니다.
oX	XML 출력을 생성합니다.

운영체제 포트

다음 표에는 NMAP가 OS 스캔에 사용하는 TCP 포트가 나와 있습니다. 또한 NMAP는 ICMP 및 UDP 포트 51824도 사용합니다.

1	3	4	6	7	9	13	17	19
20	21	22	23	24	25	26	30	32
33	37	42	43	49	53	70	79	80
81	82	83	84	85	88	89	90	99
100	106	109	110	111	113	119	125	135
139	143	144	146	161	163	179	199	211
212	222	254	255	256	259	264	280	301
306	311	340	366	389	406	407	416	417
425	427	443	444	445	458	464	465	481
497	500	512	513	514	515	524	541	543
544	545	548	554	555	563	587	593	616
617	625	631	636	646	648	666	667	668
683	687	691	700	705	711	714	720	722
726	749	765	777	783	787	800	801	808
843	873	880	888	898	900	901	902	903
911	912	981	987	990	992	993	995	999
1000	1001	1002	1007	1009	1010	1011	1021	1022
1023	1024	1025	1026	1027	1028	1029	1030	1031
1032	1033	1034	1035	1036	1037	1038	1039	1040-1100
1102	1104	1105	1106	1107	1108	1110	1111	1112
1113	1114	1117	1119	1121	1122	1123	1124	1126

1130	1131	1132	1137	1138	1141	1145	1147	1148
1149	1151	1152	1154	1163	1164	1165	1166	1169
1174	1175	1183	1185	1186	1187	1192	1198	1199
1201	1213	1216	1217	1218	1233	1234	1236	1244
1247	1248	1259	1271	1272	1277	1287	1296	1300
1301	1309	1310	1311	1322	1328	1334	1352	1417
1433	1434	1443	1455	1461	1494	1500	1501	1503
1521	1524	1533	1556	1580	1583	1594	1600	1641
1658	1666	1687	1688	1700	1717	1718	1719	1720
1721	1723	1755	1761	1782	1783	1801	1805	1812
1839	1840	1862	1863	1864	1875	1900	1914	1935
1947	1971	1972	1974	1984	1998-2010	2013	2020	2021년
2022년	2030	2033	2034	2035	2038	2040-2043	2045-2049	2065
2068	2099	2100	2103	2105-2107	2111	2119	2121	2126
2135	2144	2160	2161	2170	2179	2190	2191	2196
2200	2222	2251	2260	2288	2301	2323	2366	2381-2383
2393	2394	2399	2401	2492	2500	2522	2525	2557
2601	2602	2604	2605	2607	2608	2638	2701	2702
2710	2717	2718	2725	2800	2809	2811	2869	2875
2909	2910	2920	2967	2968	2998	3000	3001	3003
3005	3006	3007	3011	3013	3017	3030	3031	3052
3071	3077	3128	3168	3211	3221	3260	3261	3268
3269	3283	3300	3301	3306	3322	3323	3324	3325
3333	3351	3367	3369	3370	3371	3372	3389	3390
3404	3476	3493	3517	3527	3546	3551	3580	3659
3689	3690	3703	3737	3766	3784	3800	3801	3809
3814	3826	3827	3828	3851	3869	3871	3878	3880
3889	3905	3914	3918	3920	3945	3971	3986	3995
3998	4000-4006	4045	4111	4125	4126	4129	4224	4242

4279	4321	4343	4443	4444	4445	4446	4449	4550
4567	4662	4848	4899	4900	4998	5000-5004	5009	5030
5033	5050	5051	5054	5060	5061	5080	5087	5100
5101	5102	5120	5190	5200	5214	5221	5222	5225
5226	5269	5280	5298	5357	5405	5414	5431	5432
5440	5500	5510	5544	5550	5555	5560	5566	5631
5633	5666	5678	5679	5718	5730	5800	5801	5802
5810	5811	5815	5822	5825	5850	5859	5862	5877
5900-5907	5910	5911	5915	5922	5925	5950	5952	5959
5960-5963	5987-5989	5998-6007	6009	6025	6059	6100	6101	6106
6112	6123	6129	6156	6346	6389	6502	6510	6543
6547	6565-6567	6580	6646	6666	6667	6668	6669	6689
6692	6699	6779	6788	6789	6792	6839	6881	6901
6969	7000	7001	7002	7004	7007	7019	7025	7070
7100	7103	7106	7200	7201	7402	7435	7443	7496
7512	7625	7627	7676	7741	7777	7778	7800	7911
7920	7921	7937	7938	7999	8000	8001	8002	8007
8008	8009	8010	8011	8021	8022	8031	8042	8045
8080-8090	8093	8099	8100	8180	8181	8192	8193	8194
8200	8222	8254	8290	8291	8292	8300	8333	8383
8400	8402	8443	8500	8600	8649	8651	8652	8654
8701	8800	8873	8888	8899	8994	9000	9001	9002
9003	9009	9010	9011	9040	9050	9071	9080	9081
9090	9091	9099	9100	9101	9102	9103	9110	9111
9200	9207	9220	9290	9415	9418	9485	9500	9502
9503	9535	9575	9593	9594	9595	9618	9666	9876
9877	9878	9898	9900	9917	9929	9943	9944	9968
9998	9999	10000	10001	10002	10003	10004	10009	10010
10012	10024	10025	10082	10180	10215	10243	10566	10616

10617	10621	10626	10628	10629	10778	11110	11111	11967
12000	12174	12265	12345	13456	13722	13782	13783	14000
14238	14441	14442	15000	15002	15003	15004	15660	15742
16000	16001	16012	16016	16018	16080	16113	16992	16993
17877	17988	18040	18101	18988	19101	19283	19315	19350
19780	19801	19842	20000	20005	20031	20221	20222	20828
21571	22939	23502	24444	24800	25734	25735	26214	27000
27352	27353	27355	27356	27715	28201	30000	30718	30951
31038	31337	32768	32769	32770	32771	32772	32773	32774
32775	32776	32777	32778	32779	32780	32781	32782	32783
32784	32785	33354	33899	34571	34572	34573	34601	35500
36869	38292	40193	40911	41511	42510	44176	44442	44443
44501	45100	48080	49152	49153	49154	49155	49156	49157
49158	49159	49160	49161	49163	49165	49167	49175	49176
49400	49999	50000	50001	50002	50003	50006	50300	50389
50500	50636	50800	51103	51493	52673	52822	52848	52869
54045	54328	55055	55056	55555	55600	56737	56738	57294
57797	58080	60020	60443	61532	61900	62078	63331	64623
64680	65000	65129	65389					

NMAP SNMP 포트 스캔

SNMPPortsAndOS-scan 유형은 엔드포인트가 실행되는 운영체제 및 OS 버전을 스캔하고 SNMP 포트(161 및 162)가 열려 있으면 SNMP 쿼리를 트리거합니다. 처음 식별되어 알 수 없음 프로파일과 일치하는 것으로 확인된 엔드포인트를 보다 효율적으로 분류하기 위해 이 스캔 유형을 사용할 수 있습니다.

다음 NMAP 명령은 스캔 SNMP 포트를 엔드포인트 프로파일링 정책과 연결할 때 SNMP 포트(UDP 161 및 162)를 스캔합니다.

nmap -sU -p U:161,162 -oN /opt/CSCOcpm/logs/nmap.log --append-output -oX - <IP-address>

표 ***50:*** 엔드포인트 ***SNMP*** 포트 스캔을 위한 ***NMAP*** 명령

-sU	UDP를 스캔합니다.

-p <포트 범위>	지정된 포트만 스캔합니다. 예를 들어 USP 포트 161 및 162를 스캔합니다.
oN	일반 출력을 생성합니다.
oX	XML 출력을 생성합니다.
IP-address	스캔하는 엔드포인트의 IP 주소입니다.

NMAP 공통 포트 스캔

CommanPortsAndOS-scan 유형은 엔드포인트가 실행 중인 운영체제(및 OS 버전) 및 공통 포트(TCP 및 UDP)를 스캔하며 SNMP 포트는 스캔하지 않습니다. 다음 NMAP 명령은 스캔 공통 포트를 엔드포인트 프로파일링 정책과 연결할 때 공통 포트를 스캔합니다. nmap -sTU -p T:21,22,23,25,53,80,110,135,139,143,443,445,3306,3389,8080,U:53,67,68,123,135,137,138,139,161,445,500,520,631,1434,1900 -oN /opt/CSCOcpm/logs/nmap.log --append-output -oX - <IP address>

표 ***51:*** 엔드포인트 공통 포트 스캔을 위한 ***NMAP*** 명령

-sTU	TCP 연결 스캔 및 UDP 스캔 모두입니다.
-p <포트 범위>	TCP 포트(21,22,23,25,53,80,110,135,139,143, 443,445,3306,3389,8080) 및 UDP 포트 (53,67,68,123,135,137, 138,139,161,445,500,520,631,1434,1900)를 스캔합니다.
oN	일반 출력을 생성합니다.
oX	XML 출력을 생성합니다.
IP address	스캔하는 엔드포인트의 IP 주소입니다.

공통 포트

다음 표에는 NMAP가 스캔에 사용하는 공통 포트가 나와 있습니다.

표 ***52:*** 공통 포트

TCP 포트		**UDP** 포트	
포트	서비스	포트	서비스
21/tcp	ftp	53/udp	도메인
22/tcp	ssh	67/udp	dhcps
23/tcp	telnet	68/udp	dhcpc
25/tcp	smtp	123/udp	ntp
53/tcp	도메인	135/udp	msrpc
80/tcp	http	137/udp	netbios-ns

TCP 포트		UDP 포트	
포트	서비스	포트	서비스
110/tcp	pop3	138/udp	netbios-dgm
135/tcp	msrpc	139/udp	netbios-ssn
139/tcp	netbios-ssn	161/udp	snmp
143/tcp	imap	445/udp	microsoft-ds
443/tcp	https	500/udp	isakmp
445/tcp	microsoft-ds	520/udp	route
3389/tcp	ms-term-serv	1434/udp	ms-sql-m
8080/tcp	http-proxy	1900/udp	upnp

NMAP 맞춤형 포트 스캔

공용 포트 외에 맞춤형 포트를 사용(**Work Centers(**작업 센터**)** > **Profiler(**프로파일러**)** > **Policy Elements(**정책 요소**)** > **NMAP Scan Actions(NMAP** 스캔 작업**)**또는**Policy(**정책**)** > **Policy Elements(**정책 요소**)** > **Results(**결과**)** > **Profiling(**프로파일링**)** > **Network Scan (NMAP) Actions(**네트워크 스캔 **(NMAP)** 작업**)**)하여 자동 및 수동 NMAP 스캔 작업을 지정할 수 있습니다. NMAP 프로브는 열려 있는 지정된 맞춤형 포트를 통해 엔드포인트에서 속성을 수집합니다. 이러한 속성은 ISE Identities 페이지의 엔드포인트 속성 목록에서 업데이트됩니다(**Work Centers(**작업 센터**)** > **Network Access(**네트워크 액세스**)** > **Identities(ID)** > **Endpoints(**엔드포인트**)**). 각 스캔 작업에 대해 최대 10개의 UDP와 10개의 TCP 포트를 지정할 수 있습니다. 공통 포트로 지정한 것과 같은 포트 번호는 사용할 수 없습니다. 자세한 내용은 McAfee ePolicy Orchestrator를 사용하여 프로파일러 정책 구성을 참조하십시오.

NMAP 서비스 버전 정보 포함 스캔

서비스 버전 정보 포함 NMAP 프로브는 디바이스에서 실행 중인 서비스에 대한 정보를 수집하여 엔드포인트를 보다 효율적으로 분류하기 위해 자동으로 스캔합니다. 서비스 버전 옵션을 공용 포트 또는 맞춤형 포트와 결합할 수 있습니다.

예:

CLI 명령: nmap -sV -p T:8083 172.21.75.217

출력:

포트	상태	서비스	버전
8083/tcp	개방형	http	McAfee ePolicy Orchestrator 에이전트 4.8.0.1500 (ePOServerName: WIN2008EPO, AgentGuid: {15D79A24-33BA-40AE-76C2-E})

NMAP SMB 검색 스캔

그러면 NMAP SMB Discovery가 Windows 버전을 구별할 수 있으므로 엔드포인트 프로파일링을 보다 효율적으로 수행할 수 있습니다. NMAP에서 제공하는 SMB 검색 스크립트를 실행하도록 NMAP 스캔 작업을 구성할 수 있습니다.

NMAP 스캔 작업은 Windows 기본 정책 내에 통합되며, 엔드포인트가 정책 및 스캔 규칙과 일치하는 경우 엔드포인트가 스캔되고 결과를 통해 정확한 Windows 버전을 확인할 수 있습니다. 피드 서비스에서 정책이 구성되며, SMB 검색 옵션을 사용하여 사전 정의된 새 NMAP 스캔이 생성됩니다.

NMAP 스캔 작업은 Microsoft-Workstation 정책에 의해 호출되며 스캔 결과는 엔드포인트의 운영체제 속성 아래에 저장되어 Windows 정책에 활용됩니다. 서브넷의 수동 스캔에서 SMB 검색 스크립트 옵션을 찾을 수도 있습니다.

참고 SMB 검색의 경우 엔드포인트에서 Windows 파일 공유 옵션을 활성화해야 합니다.

SMB 검색 속성

엔드포인트에서 SMB 검색 스크립트가 실행되면 SMB.Operating-system과 같은 새 SMB 검색 속성이 엔드포인트에 추가됩니다. 피드 서비스에서 Windows 엔드포인트 프로파일링 정책을 업데이트할 때 이러한 속성을 고려합니다. SMB 검색 스크립트가 실행되면 SMB 검색 속성 앞에 SMB.operating-system, SMB.lanmanager, SMB.server, SMB.fqdn, SMB.domain, SMB.workgroup, SMB.cpe와 같은 SMB가 접두사로 붙습니다.

NMAP 호스트 검색 스캔 건너뛰기

모든 IP 주소의 포트를 모두 스캔하려면 시간이 많이 걸립니다. 스캔의 목적에 따라서는 활성 엔드포인트의 NMAP 호스트 검색을 건너뛸 수 있습니다.

엔드 포인트 분류 후 NMAP 스캔이 트리거되는 경우 프로파일 러는 항상 엔드 포인트의 호스트 검색을 건너 뜁니다. 그러나 Skip NMAP Host Discovery(NMAP 호스트 검색 건너뛰기)를 활성화한 후 수동 스캔 작업이 트리거되면 호스트 검색을 건너뛰게 됩니다.

NMAP 스캔 워크플로우

NMAP 스캔을 수행하기 위해 따라야 할 단계:

시작하기 전에

NMAP SMB 검색 스크립트를 실행하려면 시스템에서 파일 공유를 활성화해야 합니다. 예를 확인하려면 NMAP SMB 검색 스크립트 실행을 위해 파일 공유 활성화 항목을 참고하십시오.

단계 **1** SMB 스캔 작업 생성.

단계 **2** SMB 스캔 작업을 사용하여 프로파일러 정책 구성.

단계 **3** SMB 속성을 사용하여 새 조건 추가.

SMB 스캔 작업 생성

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Policy(**정책**)** > **Policy Elements(**정책 요소**)** > **Results(**결과**)** > **Profiling(**프로파일링**)** > **Network Scan (NMAP) Actions(**네트워크 스캔**(NMAP)** 작업**)**를 선택합니다.

단계 **2** **Action Name(**작업 이름**)** 및 **Description(**설명**)**을 입력합니다.

단계 **3** **Run SMB Discovery Script(SMB** 검색 스크립트 실행**)** 확인란을 선택합니다.

단계 **4** 네트워크 액세스 사용자를 생성하려면 **Add(**추가**)**를 클릭합니다.

다음에 수행할 작업

SMB 스캔 작업을 사용하여 프로파일러 정책을 구성해야 합니다.

SMB 스캔 작업을 사용하여 프로파일러 정책 구성

시작하기 전에

SMB 스캔 작업을 사용하여 엔드포인트를 스캔하려면 새 프로파일러 정책을 생성해야 합니다. 예를 들어 DHCP 클래스 식별자가 MSFT 속성을 포함하면 네트워크 작업을 수행해야 하는 규칙을 지정하여 Microsoft 워크스테이션을 스캔할 수 있습니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Policy(**정책**)** > **Profiling(**프로파일링**)** > **Add(**추가**)**를 선택합니다.

단계 **2** **Name(**이름**)** 및 **Description(**설명**)**을 입력합니다.

단계 **3** 드롭다운에서, 생성한 스캔 작업(예: SMBScanAction)을 선택합니다.

다음에 수행할 작업

SMB 속성을 사용하여 새 조건을 추가해야 합니다.

SMB 속성을 사용하여 새 조건 추가

시작하기 전에

엔드포인트 버전을 스캔하려면 새 프로파일러 정책을 생성해야 합니다. 예를 들어 Microsoft 워크스테이션 상위 정책 아래에서 Windows 7을 스캔할 수 있습니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Policy(**정책**)** > **Profiling(**프로파일링**)** > **Add(**추가**)**를 선택합니다.

단계 **2** **Name(**이름**)**(예: Windows-7Workstation) 및 **Description(**설명**)**을 입력합니다.

단계 **3** **Network Scan (NMAP) Action(**네트워크 스캔**(NMAP)** 작업**)** 드롭다운에서 **None(**없음**)**을 선택합니다.

단계 **4** **Parent Policy(**상위 정책**)** 드롭다운에서 Microsoft-Workstation 정책을 선택합니다.

NMAP SMB 검색 스크립트 실행을 위해 파일 공유 활성화

아래에는 NMAP SMB 검색 스크립트를 실행하기 위해 Windows OS 버전 7에서 파일 공유를 활성화하는 예가 나와 있습니다.

단계 **1** 제어판 > 네트워크 및 인터넷을 선택합니다.

단계 **2** 네트워크 및 공유 센터를 선택합니다.

단계 **3** 고급 공유 설정 변경을 선택합니다.

단계 **4** 파일 및 프린터 공유 켜기를 클릭합니다.

단계 **5** **40**비트 또는 **56**비트 암호화를 사용하는 장치에 대해 파일 공유 사용 및 비밀번호 보호 공유 켜기 옵션을 활성화합니다.

단계 **6** **Save Changes(**변경 사항 저장**)**를 클릭합니다.

단계 **7** 방화벽 설정을 구성합니다.

a) 제어판에서 시스템 및 보안 > **Windows** 방화벽 > **Windows** 방화벽에서 프로그램 허용으로 이동합니다.
b) 파일 및 프린터 공유 확인란이 선택되어 있는지 확인합니다.
c) 확인을 클릭합니다.

단계 **8** 공유 폴더를 구성합니다.

a) 대상 폴더를 마우스 오른쪽 버튼으로 클릭하고 속성을 선택합니다.
b) 공유 탭을 클릭하고 공유를 클릭합니다.
c) 파일 공유 대화 상자에서 필요한 이름을 추가하고 공유를 클릭합니다.
d) 선택한 폴더를 공유한 후 완료를 클릭합니다.
e) 고급 공유를 클릭하고 이 폴더 공유 확인란을 선택합니다.
f) 권한을 클릭합니다.
g) 스캔 권한 대화 상자에서 **Everyone**을 선택하고 모든 권한 확인란을 선택합니다.
h) **OK(**확인**)**를 클릭합니다.

NMAP 스캔에서 서브넷 제외

NMAP 스캔을 수행하여 엔드포인트의 OS 또는 SNMP 포트를 식별할 수 있습니다.

NMAP 스캔을 수행할 때 NMAP에서 스캔하지 않아야 하는 전체 서브넷 또는 IP 범위를 제외할 수 있습니다. **NMAP Scan Subnet Exclusions(NMAP** 스캔 서브넷 제외**)** 창(**Work Centers(**작업 센터**) > Profiler(**프로파일러**) > Settings(**설정**) > NMAP Scan Subnet Exclusions(NMAP** 스캔 서브넷 제외**)**)에서 서브넷 또는 IP 범위를 구성할 수 있습니다. 이렇게 하면 네트워크의 로드를 제한하고 상당한 시간을 절약할 수 있습니다.

수동 NMAP 스캔의 경우 **Run Manual NMAP Scan(**수동 **NMAP** 스캔 실행**)** 창(**Work Centers(**작업 센터**) > Profiler(**프로파일러**) > Manual Scans(**수동 스캔**) > Manual NMAP Scan(**수동 **NMAP** 스캔**) >**

Configure NMAP Scan Subnet Exclusions(NMAP 스캔 서브넷 제외 구성**)**)을 사용하여 서브넷 또는 IP 범위를 지정할 수 있습니다.

수동 NMAP 스캔 설정

자동 NMAP 스캔에 사용할 수 있는 스캔 옵션을 사용하여 수동 NMAP 스캔(**Work Centers(**작업 센터**)** > **Profiler(**프로파일러**)** > **Manual Scans(**수동 스캔**)** > **Manual NMAP Scan(**수동 **NMAP** 스캔**)**)을 수행할 수 있습니다. 스캔 옵션 또는 사전 정의된 스캔을 선택할 수 있습니다.

표 ***53:*** 수동 ***NMAP*** 스캔 설정

필드 이름	사용 지침
Node(노드**)**	NMAP 스캔이 실행되는 ISE 노드를 선택합니다.
Manual Scan Subnet(수동 스캔 서브넷**)**	NMAP 스캔을 실행할 엔드포인트의 서브넷 IP 주소 범위를 입력합니다.
Configure NMAP Scan Subnet Exclusions At(다음 위치에서 **NMAP** 스캔 서브넷 제외 구성**)**	**Work Centers(**작업 센터**)** > **Profiler(**프로파일러**)** > **Settings(**설정**)** > **NMAP Scan Subnet Exclusions(NMAP** 스캔 서브넷 제외**)** 창으로 이동됩니다. 제외할 IP 주소 및 서브넷 마스크를 지정합니다. 일치하는 항목이 있으면 NMAP 스캔은 실행되지 않습니다.
NMAP Scan Subnet(NMAP 스캔 서브넷**)**	다음 중 하나를 수행할 수 있습니다. • Specify Scan Options(스캔 옵션 지정) • Select an Existing NMAP Scan(기존 NMAP 스캔 선택)
Specify Scan Options(스캔 옵션 지정**)**	필수 스캔 옵션인 OS, SNMP Port(SNMP 포트), Common Ports(공용 포트), Custom Ports(맞춤형 포트), Include Service Version Information(서비스 버전 정보 포함), Run SMB Discovery Script(SMB 검색 스크립트 실행), Skip NMAP Host Discovery(NMAP 호스트 검색 건너뛰기)를 선택합니다. 자세한 내용은 네트워크 스캔 작업 생성을 참고하십시오.
Select an Existing NMAP Scan(기존 **NMAP** 스캔 선택**)**	기본 프로파일러 NMAP 스캔 작업이 표시되는 **Existing NMAP Scan Actions(**기존 **NMAP** 스캔 작업**)** 드롭다운 목록을 표시합니다.
Reset to Default Scan Options(기본 스캔 옵션으로 재설정**)**	기본 설정으로 되돌리려면 이 옵션을 클릭합니다(모든 스캔 옵션이 선택됨).

필드 이름	사용 지침
Save as NMAP Scan Action(NMAP 스캔 작업으로 저장**)**	작업 이름과 설명을 입력합니다.

수동 **NMAP** 스캔 실행

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Profiler(**프로파일러**)** > **Manual Scans(**수동 스캔**)** > **Manual NMAP Scan(**수동 **NMAP** 스캔**)**을 선택합니다.

단계 **2** **Node(**노드**)** 드롭다운 목록에서 NMAP 스캔을 실행하려는 ISE 노드를 선택합니다.

단계 **3** **Manual Scan Subnet(**수동 스캔 서브넷**)** 텍스트 상자에서 열린 포트를 확인하려는 엔드포인트가 있는 서브넷 주소를 입력합니다.

단계 **4** 다음 중 하나를 선택합니다.

a) **Specify Scan Options(**스캔 옵션 지정**)**를 선택하고 페이지 오른쪽에서 필요한 스캔 옵션을 선택합니다. 자세한 내용은 네트워크 스캔 작업 생성 페이지를 참고하십시오.

b) **Select An Existing NMAP Scan Action(**기존 **NMAP** 스캔 작업 선택**)**을 선택하고 MCAFeeEPOOrchestratorClientScan과 같은 기본 NMAP 스캔 작업을 선택합니다.

단계 **5** **Run Scan(**스캔 실행**)**을 클릭합니다.

McAfee ePolicy Orchestrator를 사용하여 프로파일러 정책 구성

Cisco ISE 프로파일링 서비스는 McAfee ePO(McAfee ePolicy Orchestrator) 클라이언트가 엔드포인트에 있는지를 탐지할 수 있습니다. 이렇게 하면 지정된 엔드포인트가 조직에 속하는지 확인하는 데 도움이 됩니다.

프로세스와 관련된 엔터티는 다음과 같습니다.

- ISE 서버
- McAfee ePO 서버
- McAfee ePO 에이전트

Cisco ISE는 구성된 포트에서 NMAP McAfee 스크립트를 사용하여 엔드포인트에서 McAfee 에이전트가 실행되고 있는지를 확인하기 위해 기본 제공 NMAP 스캔 작업(MCAFeeEPOOrchestratorClientscan)을 제공합니다. 맞춤형 포트(예: 8082)를 사용하여 새 NMAP 스캔 옵션을 생성할 수도 있습니다. 아래 단계에 따라 McAfee ePO 소프트웨어를 사용하는 새 NMAP 스캔 작업을 구성할 수 있습니다.

단계 **1** McAfee ePo NMAP 스캔 작업 구성.

단계 **2** McAfee ePO 에이전트 구성.

단계 **3** McAfee ePO NMAP 스캔 작업을 사용하여 프로파일러 정책 구성.

McAfee ePo NMAP 스캔 작업 구성

단계 1 Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Profiler(**프로파일러**)** > **Policy Elements(**정책 요소**)** > **Network Scan (NMAP) Actions(**네트워크 스캔**(NMAP)** 작업**)**를 선택합니다.

단계 2 **Add(**추가**)**를 클릭합니다.

단계 3 작업 이름 및 설명을 입력합니다.

단계 4 **Scan Options(**스캔 옵션**)**에서 **Custom Ports(**맞춤형 포트**)**를 선택합니다.

단계 5 **Custom Ports(**맞춤형 포트**)** 대화 상자에서 필요한 TCP 포트를 추가합니다. McAfee ePO용으로는 기본적으로 8080 TCP 포트가 활성화됩니다.

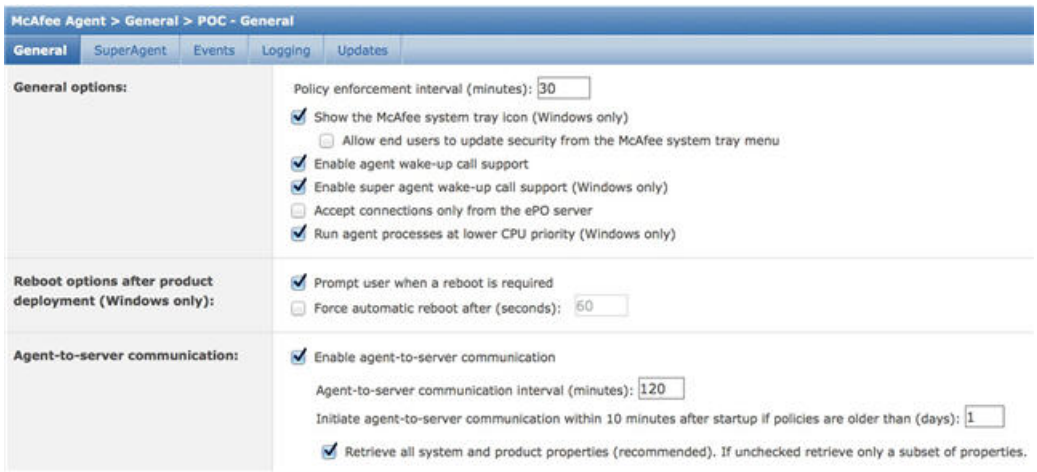
단계 6 **Include Service Version Information(**서비스 버전 정보 포함**)** 확인란을 선택합니다.

단계 7 **Submit(**제출**)**을 클릭합니다.

McAfee ePO 에이전트 구성

단계 1 McAfee ePO 서버에서 McAfee ePO 에이전트와 ISE 서버 간의 통신을 원활하게 수행하기 위한 권장 설정을 선택합니다.

그림 ***15: McAfee ePO*** 에이전트 권장 옵션



단계 2 **Accept Connections Only From The ePO Server(ePO** 서버로부터의 연결만 수락**)**이 선택 취소되어 있는지 확인합니다.

McAfee ePO NMAP 스캔 작업을 사용하여 프로파일러 정책 구성

단계 1 Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Policy(**정책**)** > **Profiling(**프로파일링**)** > **Add(**추가**)**를 선택합니다.

단계 2 **Name(**이름**)** 및 **Description(**설명**)**을 입력합니다.

단계 **3** **Network Scan (NMAP) Action(**네트워크 스캔**(NMAP)** 작업**)** 드롭다운 목록에서 필요한 작업(예: MCAFeeEPOOrchestratorClientscan)을 선택합니다.

단계 **4** 상위 프로파일러 정책을 생성합니다(예: DHCP 클래스 식별자가 MSFT 속성을 포함하는지를 확인하는 규칙이 들어 있는 Microsoft-Workstation).

단계 **5** 엔드포인트에 McAfee ePO 에이전트가 설치되어 있는지를 확인하기 위해 상위 NMAP McAfee ePO 정책(예: Microsoft-Workstation) 내에 새 정책(예: CorporateDevice)을 생성합니다.

조건을 충족하는 엔드포인트는 기업 디바이스로 프로파일링됩니다. 정책을 사용하여 McAfee ePO 에이전트로 프로파일링된 엔드포인트를 새 VLAN으로 이동할 수 있습니다.

프로파일러 엔드포인트 사용자 맞춤화 속성

엔드포인트가 프로브에서 수집하는 속성 외에 엔드포인트에 속성을 할당하려면 **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **Settings(**설정**)** > **Endpoint Custom Attributes(**엔드포인트 사용자 맞춤화 속성**)**를 선택합니다. 엔드포인트 사용자 맞춤화 속성은 권한 부여 정책에서 엔드포인트를 프로파일링하는 데 사용될 수 있습니다.

최대 100개의 엔드포인트 사용자 맞춤화 속성을 생성할 수 있습니다. 지원되는 엔드포인트 사용자 맞춤화 속성 유형은 정수, 문자열, 정수(Long), 부울 및 부동 소수점입니다.

Context Directory(상황 디렉터리**)** > **Endpoints(**엔드포인트**)** > **Endpoint Classification(**엔드포인트 분류**)** 창에서 엔드포인트 사용자 맞춤화 속성의 값을 추가할 수 있습니다.

엔드포인트 사용자 맞춤화 속성의 활용 사례에는 특정 속성에 따라 디바이스를 허용 또는 차단하거나 권한 부여에 따라 특정 권한을 할당하는 것이 포함됩니다.

권한 부여 정책에서 엔드포인트 사용자 맞춤화 속성 사용

Endpoint Custom Attributes(엔드포인트 사용자 맞춤화 속성) 섹션에서는 추가 속성을 구성할 수 있습니다. 각 정의는 속성 및 유형(문자열, 정수, 부울, 부동, Long)으로 구성됩니다. 사용자 맞춤화 속성을 사용하여 디바이스를 프로파일링할 수 있습니다.

참고 엔드포인트에 사용자 맞춤화 속성을 추가하려면 Cisco ISE Advantage 라이선스가 있어야 합니다.

다음 단계에서는 엔드포인트 사용자 맞춤화 속성을 사용하여 권한 부여 정책을 생성하는 방법을 보여줍니다.

단계 **1** 엔드포인트 사용자 맞춤화 속성을 생성하고 값을 할당합니다.

a) **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **Settings(**설정**)** > **Endpoint Custom Attributes(**엔드포인트 맞춤형 속성**)** 페이지를 선택합니다.

b) **Endpoint Custom Attributes(**엔드포인트 사용자 맞춤화 속성**)** 영역에서 **Attribute Name(**속성 이름**)**(예: deviceType), Data Type(데이터 유형)(예: String(문자열)) 및 Parameters(파라미터)를 입력합니다.

c) **Save(**저장**)**를 클릭합니다.

d) **Context Visibility(**상황 가시성**)** > **Endpoints(**엔드포인트**)** > **Summary(**요약**)**를 선택합니다.

e) 맞춤형 속성 값을 할당합니다.

- 필요한 MAC 주소 확인란을 선택하고 **Edit(**편집**)**를 클릭합니다.
- 또는 필요한 MAC 주소를 클릭하고 Endpoints(엔드포인트) 페이지에서 **Edit(**편집**)**를 클릭합니다.

f) **Edit Endpoint(**엔드포인트 편집**)** 대화 상자의 **Custom Attribute(**맞춤형 속성**)** 영역에서 필요한 속성 값(예: deviceType = Apple-iPhone)을 입력합니다.

g) **Save(**저장**)**를 클릭합니다.

단계 **2** 맞춤형 속성 및 값을 사용하여 권한 부여 정책을 생성합니다.

a) **Policy(**정책**)** > **Policy Sets(**정책 집합**)**를 선택합니다.

b) Endpoints(엔드포인트) 사전에서 맞춤형 속성(예: Rule Name: Corporate Devices, Conditions:EndPoints:deviceType Contains Apple-iPhone, Permissions: then PermitAccess)을 선택하여 권한 부여 정책을 생성합니다.

c) **Save(**저장**)**를 클릭합니다.

관련 항목

프로파일러 엔드포인트 사용자 맞춤화 속성, 229 페이지

프로파일러 조건 생성

Cisco ISE의 엔드포인트 프로파일링 정책을 사용하면 네트워크에서 검색된 엔드포인트를 분류하여 특정 엔드포인트 ID 그룹에 할당할 수 있습니다. 이러한 엔드포인트 프로파일링 정책은 Cisco ISE가 엔드포인트를 분류하고 그룹화하기 위해 평가하는 프로파일링 조건으로 구성됩니다.

시작하기 전에

다음 작업을 수행하려면 슈퍼 관리자 또는 정책 관리자여야 합니다.

단계 **1** **Policy(**정책**)** > **Policy Elements(**정책 요소**)** > **Conditions(**조건**)** > **Profiling(**프로파일링**)** > **Add(**추가**)**를 선택합니다.

단계 **2** 엔드포인트 프로파일링 정책 설정, 231 페이지의 설명에 따라 필드의 값을 입력합니다.

단계 **3** 프로파일러 조건을 저장하려면 **Submit(**제출**)**을 클릭합니다.

단계 **4** 조건을 더 생성하려면 이 절차를 반복합니다.

엔드포인트 프로파일링 정책 규칙

라이브러리에서 이전에 생성하여 정책 요소 라이브러리에 저장한 프로파일링 조건 중 하나 이상을 선택할 수 있도록 하는 규칙을 정의할 수 있습니다. 또한 그러한 규칙에 따라 각 조건의 확실성 요인에 대한 정수 값을 연결하거나 해당 조건에 대해 예외 작업 또는 네트워크 스캔 작업을 연결할 수도

있습니다. 예외 작업 또는 네트워크 스캔 작업은 구성 가능한 작업을 트리거하는 데 사용되지만 Cisco ISE는 엔드포인트의 전반적인 분류에 따라 프로파일링 정책을 평가합니다.

OR 연산자를 사용하여 지정된 정책의 규칙을 개별적으로 평가하는 경우 각 규칙의 확실성 메트릭은 엔드포인트 프로파일을 전반적으로 특정 엔드포인트 범주와 일치시키는 데 사용됩니다. 엔드포인트 프로파일링 정책의 규칙이 일치하는 경우 네트워크에서 동적으로 검색되는 프로파일링 정책 및 일치하는 정책은 엔드포인트에 대해 동일합니다.

규칙에서 논리적으로 그룹화된 조건

엔드포인트 프로파일링 정책(프로파일)에는 단일 조건 또는 여러 단일 조건 조합이 포함되어 있으며 그러한 조건은 AND 또는 OR 연산자를 사용하여 논리적으로 결합될 수 있습니다. 이 조건을 기준으로 정책에서 지정된 규칙과 비교하여 엔드포인트를 확인, 분류 및 그룹화할 수 있습니다.

조건은 엔드포인트의 조건에 지정된 값과 비교하여 수집된 엔드포인트 속성 값을 확인하는 데 사용됩니다. 여러 속성을 매핑하는 경우 조건을 논리적으로 그룹화할 수 있습니다. 그러면 네트워크의 엔드포인트를 분류하는 데 도움이 됩니다. 규칙에서 연결되어 있는 해당 확실성 메트릭(정의한 정수 값)을 사용하여 그러한 하나 이상의 조건과 비교하여 엔드포인트를 확인할 수 있습니다. 또는 조건에 연결된 예외 작업이나 조건에 연결된 네트워크 스캔 작업을 트리거할 수 있습니다.

확실성 요인

프로파일링 정책의 최소 확실성 메트릭은 엔드포인트에 대해 일치하는 프로파일을 평가합니다. 엔드포인트 프로파일링 정책의 각 규칙에는 프로파일링 조건에 연결된 최소 확실성 메트릭(정수 값)이 있습니다. 확실성 메트릭은 엔드포인트 프로파일링 정책의 모든 유효한 규칙에 대해 추가되는 수단으로, 엔드포인트 프로파일링 정책의 각 조건이 엔드포인트의 전반적인 분류를 향상시키는 데 어떤 영향을 미치는지 측정합니다.

각 규칙의 확실성 메트릭은 엔드포인트 프로파일을 전반적으로 특정 엔드포인트 범주와 일치시키는 데 사용됩니다. 모든 유효한 규칙의 확실성 메트릭은 함께 추가되어 일치하는 확실성을 이룹니다. 이는 엔드포인트 프로파일링 정책에 정의된 최소 확실성 요인보다 높아야 합니다. 기본적으로 모든 새로운 프로파일링 정책 규칙 및 미리 정의된 프로파일링 정책에 대한 최소 확실성 요인은 10입니다.

엔드포인트 프로파일링 정책 설정

다음 표에서는 **Endpoint Policies(**엔드포인트 정책**)** 창의 필드에 대해 설명합니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Policy(**정책**)** > **Profiling(**프로파일링**)** > **Profiling Policies(**프로파일링 정책**)**입니다.

표 ***54:*** 엔드포인트 프로파일링 정책 설정

필드 이름	사용 지침
Name(이름**)**	생성하려는 엔드포인트 프로파일링 정책의 이름을 입력합니다.
Description(설명**)**	생성하려는 엔드포인트 프로파일링 정책의 설명을 입력합니다.

필드 이름	사용 지침
Policy Enabled(정책 활성화**)**	엔드포인트를 프로파일링할 때 일치하는 프로파일링 정책을 연결하기 위해 **Policy Enabled(**정책 활성화**)** 확인란은 기본적으로 선택됩니다. 이 확인란의 선택을 취소하면 엔드포인트 프로파일링 시 엔드포인트 프로파일링 정책이 제외됩니다.
Minimum Certainty Factor(최소 확실성 요인**)**	프로파일링 정책과 연결할 최소값을 입력합니다. 기본값은 10입니다.
Exception Action(예외 작업**)**	프로파일링 정책에서 규칙을 정의할 때 조건과 연결할 예외 작업을 선택합니다. 기본값은 NONE(없음)입니다. **Policy(**정책**) > Policy Elements(**정책 요소**) > Results(**결과**) > Profiling(**프로파일링**) > Exception Actions(**예외 작업**)**에서 예외 작업을 정의합니다.
Network Scan (NMAP) Action(네트워크 스캔 **(NMAP)** 작업**)**	필요한 경우 프로파일링 정책에서 규칙을 정의할 때 조건과 연결할 네트워크 스캔 작업을 목록에서 선택합니다. 기본값은 NONE(없음)입니다. **Policy(**정책**) > Policy Elements(**정책 요소**) > Results(**결과**) > Profiling(**프로파일링**) > Network Scan (NMAP) Actions(**네트워크 스캔**(NMAP)** 작업**)**에서 예외 작업을 정의합니다.
Create an Identity Group for the policy(정책에 대한 **ID** 그룹 생성**)**	엔드포인트 ID 그룹을 생성하려면 다음 옵션 중 하나를 선택합니다. • **Yes, create matching Identity Group(**예**,** 일치하는 **ID** 그룹을 생성합니다**.)** • **No, use existing Identity Group hierarchy(**아니요**,** 기존 **ID** 그룹 계층을 사용합니다**.)**

필드 이름	사용 지침
Yes, create matching Identity Group(예**,** 일치하는 **ID** 그룹을 생성합니다**.)**	기존 프로파일링 정책을 사용하려면 이 옵션을 선택합니다. 이 옵션을 선택하면 해당 엔드포인트에 대해 일치하는 ID 그룹이 생성되며, 엔드포인트 프로파일이 기존 프로파일링 정책과 일치하면 ID 그룹은 Profiled 엔드포인트 ID 그룹의 자식이 됩니다. 예를 들어 네트워크에서 검색된 엔드포인트가 Xerox-Device 프로파일과 일치하면 엔드포인트 ID 그룹 페이지에서 Xerox-Device 엔드포인트 ID 그룹이 생성됩니다.
No, use existing Identity Group hierarchy(아니요**,** 기존 **ID** 그룹 계층을 사용합니다**.)**	프로파일링 정책 및 ID 그룹의 계층 구성을 사용하여 일치하는 부모 엔드포인트 ID 그룹에 엔드포인트를 할당하려면 이 확인란을 선택합니다. 이 옵션을 사용하는 경우 엔드포인트 프로파일링 정책 계층을 사용하여 일치하는 부모 엔드포인트 ID 그룹 중 하나와 부모 ID 그룹에 대해 연결된 엔드포인트 ID 그룹에 엔드포인트를 할당할 수 있습니다. 예를 들어 기존 프로파일과 일치하는 엔드포인트는 적절한 부모 엔드포인트 ID 그룹 아래에 그룹화됩니다. 여기서 Unknown(알 수 없음) 프로파일과 일치하는 엔드포인트는 Unknown(알 수 없음) 아래에 그룹화되고 기존 프로파일과 일치하는 엔드포인트는 프로파일이 지정된 엔드포인트 ID 그룹 아래에 그룹화됩니다. 예를 들면 다음과 같습니다. • Cisco-IP-Phone 프로파일과 일치하는 엔드포인트는 Cisco-IP-Phone 엔드포인트 ID 그룹 아래에 그룹화됩니다. • Workstation 프로파일과 일치하는 엔드포인트는 Workstation 엔드포인트 ID 그룹 아래에 그룹화됩니다. Cisco-IP-Phone 및 Workstation 엔드포인트 ID 그룹은 시스템의 Profiled 엔드포인트 ID 그룹에 연결됩니다.

필드 이름	사용 지침
Parent Policy(부모 정책**)**	새 엔드포인트 프로파일링 정책을 연결할 시스템에 정의된 부모 프로파일링 정책을 선택합니다. 자식에게 규칙과 조건을 상속할 부모 프로파일링 정책을 선택할 수 있습니다.
Associated CoA Type(연결된 **CoA** 유형**)**	엔드포인트 프로파일링 정책과 연결할 CoA 유형을 다음 중에서 하나 선택합니다. • CoA 없음 • 포트 바운스 • 재인증 • Administration(관리) > System(시스템) > Settings(설정) > Profiling(프로파일링)에 설정된 프로파일러 컨피그레이션에서 적용되는 전역 설정
Rules(규칙**)**	엔드포인트 프로파일링 정책에 정의된 하나 이상의 규칙에 따라 엔드포인트에 일치하는 프로파일링 정책이 결정됩니다. 그러면 해당 프로파일에 따라 엔드포인트를 그룹화할 수 있습니다. 규칙에서는 정책 요소 라이브러리의 프로파일링 조건을 하나 이상 사용하여 전체 분류를 위한 엔드포인트 속성 및 해당 값을 검증합니다.

필드 이름	사용 지침
Conditions(조건**)**	고정된 Conditions(조건) 오버레이를 확장하려면 더하기 [+] 기호를 클릭하고, 고정된 오버레이를 닫으려면 빼기 [-] 기호를 클릭하거나 오버레이 바깥쪽을 클릭합니다. **Select Existing Condition from Library(**라이브러리에서 기존 조건 선택**)** 또는 **Create New Condition (Advanced Option)(**새 조건 생성**(**고급 옵션**))**을 클릭합니다. **Select Existing Condition from Library(**라이브러리에서 기존 조건 선택**)**: 정책 요소 라이브러리에서 미리 정의된 Cisco 조건을 선택하여 식을 정의할 수 있습니다. **Create New Condition (Advanced Option)(**새 조건 생성**(**고급 옵션**))**: 여러 시스템 또는 사용자 맞춤화 사전에서 속성을 선택하여 식을 정의할 수 있습니다. 다음 중 하나를 프로파일링 조건과 연결할 수 있습니다. • 각 조건에 대한 확실성 요인의 정수 값 • 해당 조건에 대한 예외 작업 또는 네트워크 스캔 작업 프로파일링 조건과 연결할 다음의 미리 정의된 설정 중 하나를 선택합니다. • Certainty Factor Increases(확실성 요인 증가): 각 규칙에 대한 확실성 값을 입력합니다. 전체 분류와 관련하여 모든 일치 규칙에 대해 이 값을 추가할 수 있습니다. • Take Exception Action(예외 작업 수행): 이 엔드포인트 프로파일링 정책의 Exception Action(예외 작업) 필드에 구성되어 있는 예외 작업을 트리거합니다. • Take Network Scan Action(네트워크 스캔 작업 수행): 이 엔드포인트 프로파일링 정책의 Network Scan (NMAP) Action(네트워크 스캔 (NMAP) 작업) 필드에 구성되어 있는 네트워크 스캔 작업을 트리거합니다.

필드 이름	사용 지침
Select Existing Condition from Library(라이브러리에서 기존 조건 선택**)**	다음을 수행할 수 있습니다. • 정책 요소 라이브러리에서 사용 가능한 미리 정의된 Cisco 조건을 선택한 다음 AND 또는 OR 연산자를 사용하여 여러 조건을 추가할 수 있습니다. • Action(작업) 아이콘을 클릭하여 후속 단계에서 다음을 수행합니다. • **Add Attribute or Value(**속성 또는 값 추가**)**: 임시 속성 또는 값 쌍을 추가할 수 있습니다. • **Add Condition from Library(**라이브러리에서 조건 추가**)**: 미리 정의된 Cisco 조건을 추가할 수 있습니다. • **Duplicate(**복제**)**: 선택한 조건의 복사본을 생성합니다. • **Add Condition to Library(**라이브러리에 조건 추가**)**: 생성한 임시 속성/값 쌍을 정책 요소 라이브러리에 저장할 수 있습니다. • **Delete(**삭제**)**: 선택한 조건을 삭제합니다.

필드 이름	사용 지침
Create New Condition (Advance Option)(새 조건 생성**(**고급 옵션**))**	다음을 수행할 수 있습니다. • 식에 임시 속성/값 쌍을 추가한 다음 AND 또는 OR 연산자를 사용하여 여러 조건을 추가할 수 있습니다. • Action(작업) 아이콘을 클릭하여 후속 단계에서 다음을 수행합니다. • **Add Attribute or Value(**속성 또는 값 추가**)**: 임시 속성 또는 값 쌍을 추가할 수 있습니다. • **Add Condition from Library(**라이브러리에서 조건 추가**)**: 미리 정의된 Cisco 조건을 추가할 수 있습니다. • **Duplicate(**복제**)**: 선택한 조건의 복사본을 생성합니다. • **Add Condition to Library(**라이브러리에 조건 추가**)**: 생성한 임시 속성/값 쌍을 정책 요소 라이브러리에 저장할 수 있습니다. • **Delete(**삭제**)**: 선택한 조건을 삭제합니다. AND 또는 OR 연산자를 사용할 수 있습니다.

관련 항목

Cisco ISE 프로파일링 서비스, 186 페이지
엔드포인트 프로파일링 정책 생성, 237 페이지
UDID 속성을 사용하는 엔드포인트 상황 가시성, 274 페이지

엔드포인트 프로파일링 정책 생성

새 프로파일러 정책 페이지에서 다음 옵션을 사용하여 프로파일 엔드포인트에 대해 새 프로파일링 정책을 생성할 수 있습니다.

- Policy Enabled(정책 활성화)
- Create an Identity Group for the policy to create a matching endpoint identity group or use the endpoint identity group hierarchy(정책에 대해 ID 그룹을 생성하여 일치하는 엔드포인트 ID 그룹을 생성하거나 엔드포인트 ID 그룹 계층 사용)
- Parent Policy(부모 정책)

- Associated CoA Type(연결된 CoA 유형)

참고 **Profiling Policies(**프로파일링 정책**)** 창에서 엔드포인트 정책을 생성하도록 선택하는 경우 웹 브라우저에서 Stop(중지) 버튼을 사용하지 마십시오. Stop(중지) 버튼을 사용하는 경우 **New Profiler Policy(**새 프로파일러 정책**)** 창 로드가 중지되고, 다른 목록 페이지에 액세스할 때 해당 페이지 및 페이지 내의 메뉴가 로드되며, 목록 페이지 내의 Filter(필터) 메뉴를 제외한 모든 메뉴에서 작업을 수행할 수 없게 됩니다. 목록 페이지 내의 모든 메뉴에서 작업을 수행하려면 Cisco ISE에서 로그아웃했다가 다시 로그인해야 할 수 있습니다.

엔드포인트 프로파일링 정책을 복제하여 비슷한 특성의 프로파일링 정책을 생성할 수 있습니다. 이 경우 모든 조건을 재정의하여 새 프로파일링 정책을 생성하는 대신 기존 프로파일링 정책을 수정할 수 있습니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Policy(**정책**)** > **Profiling(**프로파일링**)** > **Profiling Policies(**프로파일링 정책**)**를 선택합니다.

단계 **2** **Add(**추가**)**를 클릭합니다.

단계 **3** 생성하려는 새 엔드포인트 정책의 이름과 설명을 입력합니다. 엔드포인트를 프로파일링할 때 검증용으로 엔드포인트 프로파일링 정책을 포함하기 위해 **Policy Enabled(**정책 활성화**)** 확인란은 기본적으로 선택됩니다.

단계 **4** 유효한 범위(1~65,535) 내의 최소 확실성 요인 값을 입력합니다.

단계 **5** **Exception Action(**예외 작업**)** 드롭다운 목록 옆의 화살표를 클릭하여 예외 작업을 연결하거나, **Network Scan (NMAP) Action(**네트워크 스캔**(NMAP)** 작업**)** 드롭다운 목록 옆의 화살표를 클릭하여 네트워크 스캔 작업을 연결합니다.

단계 **6** **Create an Identity Group for the policy(**정책에 대한 **ID** 그룹 생성**)**에 대해 다음 옵션 중 하나를 선택합니다.

- **Yes, create matching Identity Group(**예**,** 일치하는 **ID** 그룹을 생성합니다**.)**
- **No, use existing Identity Group hierarchy(**아니요**,** 기존 **ID** 그룹 계층을 사용합니다**.)**

단계 **7** **Parent Policy(**부모 정책**)** 드롭다운 목록 옆의 화살표를 클릭하여 부모 정책을 새 엔드포인트 정책에 연결합니다.

단계 **8** **Associated CoA Type(**연결된 **CoA** 유형**)** 드롭다운 목록에서 연결할 CoA 유형을 선택합니다.

단계 **9** 규칙을 클릭하여 조건을 추가하고 각 조건에 대해 확실성 요인의 정수 값을 연결하거나, 엔드포인트의 전체 분류를 위해 해당 조건에 대한 예외 작업 또는 네트워크 스캔 작업을 연결합니다.

단계 **10** **Submit(**제출**)**을 클릭하여 엔드포인트 정책을 추가하거나 New Profiler Policy(새 프로파일러 정책) 페이지에서 **Profiler Policy List(**프로파일러 정책 목록**)** 링크를 클릭하여 Profiling Policies(프로파일링 정책) 페이지로 돌아갑니다.

엔드포인트 프로파일링 정책별 **CoA(Change of Authorization)** 컨피그레이션

Cisco ISE에서 CoA(Change of Authorization) 유형의 전역 컨피그레이션 외에, 각 엔드포인트 프로파일링 정책에 연결된 특정 CoA 유형을 실행하도록 구성할 수도 있습니다.

전역 No CoA(CoA 없음) 유형 컨피그레이션은 엔드포인트 프로파일링 정책에 구성된 각 CoA 유형을 재정의합니다. 전역 CoA 유형을 No CoA(CoA 없음) 유형이 아닌 다른 유형으로 설정하는 경우 각 엔드포인트 프로파일링 정책은 전역 CoA 컨피그레이션을 재정의할 수 있습니다.

CoA가 트리거되면 각 엔드포인트 프로파일링 정책에서 다음과 같이 실제 CoA 유형을 결정할 수 있습니다.

- General Setting(일반 설정) - 이는 전역 컨피그레이션별로 CoA를 실행하는 모든 엔드포인트 프로파일링 정책에 대한 기본 설정입니다.
- No CoA(CoA 없음) - 이 설정은 프로파일에 대한 전역 컨피그레이션을 재정의하고 CoA를 비활성화합니다.
- Port Bounce(포트 바운스) - 이 설정은 전역 포트 바운스 및 재인증 컨피그레이션 유형을 재정의하고 포트 바운스 CoA를 실행합니다.
- Reauth(재인증) - 이 설정은 전역 포트 바운스 및 재인증 컨피그레이션 유형을 재정의하고 재인증 CoA를 실행합니다.

참고 프로파일러 전역 CoA 컨피그레이션이 Port Bounce(포트 바운스)(또는 Reauth(재인증))로 설정된 경우, 모바일 디바이스에 대한 BYOD 흐름이 차단되지 않도록 정책 단위 CoA 옵션인 No CoA(CoA 없음)을 사용하여 해당 엔드포인트 프로파일링 정책을 구성해야 합니다.

모든 CoA 유형, 그리고 전역 및 엔드포인트 프로파일링 정책 설정에 따라 각각 발급되는 실제 CoA 유형에 대해 아래와 같이 결합된 컨피그레이션 요약을 참고해 주십시오.

표 ***55:*** 다양한 컨피그레이션 조합으로 발급되는 ***CoA*** 유형

전역 **CoA** 유형	정책별 기본 **CoA** 유형 집합	정책별 **No CoA(CoA 없음)** 유형	정책별 **Port Bounce(포트 바운스)** 유형	정책별 **Reauth(재인증)** 유형
No CoA(CoA 없음)	No CoA(CoA 없음)	No CoA(CoA 없음)	No CoA(CoA 없음)	CoA 없음
포트 바운스	Port Bounce(포트 바운스)	CoA 없음	포트 바운스	Re-Auth(재인증)
Reauth(재인증)	Reauth(재인증)	CoA 없음	포트 바운스	Re-Auth(재인증)

엔드포인트 프로파일링 정책 가져오기

내보내기 기능에서 생성할 수 있는 것과 같은 형식을 사용하여 XML로 된 파일에서 엔드포인트 프로파일링 정책을 가져올 수 있습니다. 부모 정책이 연결되어 있는 새로 생성한 프로파일링 정책을 가져오는 경우에는 자식 정책을 정의하기 전에 부모 정책을 정의해야 합니다.

가져오는 파일에는 엔드포인트 프로파일링 정책의 계층이 들어 있으며, 이 계층에는 부모 정책과 그 다음에 가져온 프로파일이 순서대로 포함되어 있고 정책에 정의된 규칙 및 확인 항목도 있습니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Policy(**정책**)** > **Profiling(**프로파일링**)** > **Profiling(**프로파일링**)** > **Profiling Policies(**프로파일링 정책**)**을 선택합니다.

단계 **2** **Import(**가져오기**)**를 클릭합니다.

단계 **3** **Browse(**찾아보기**)**를 클릭하여 이전에 내보냈으며 가져오려는 파일을 찾습니다.

단계 **4** **Submit(**제출**)**을 클릭합니다.

단계 **5** **Profiling Policies(**프로파일링 정책**)** 창으로 돌아가려면 **Profiler Policy List(**프로파일러 정책 목록**)** 링크를 클릭합니다.

엔드포인트 프로파일링 정책 내보내기

엔드포인트 프로파일링 정책을 다른 Cisco ISE 구축으로 내보낼 수 있습니다. XML 파일을 템플릿으로 사용하여 가져오려는 고유한 정책을 생성할 수도 있습니다. 또한 나중에 가져오기에 사용할 수 있도록 시스템의 기본 위치에 파일을 다운로드할 수도 있습니다.

엔드포인트 프로파일링 정책을 내보낼 때는 적절한 애플리케이션을 사용하여 profiler_policies.xml을 열거나 저장하라는 메시지가 포함된 대화 상자가 나타납니다. 이 파일은 웹 브라우저 또는 적절한 기타 애플리케이션에서 열 수 있는 XML 형식 파일입니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Policy(**정책**)** > **Profiling(**프로파일링**)** > **Profiling(**프로파일링**)** > **Profiling Policies(**프로파일링 정책**)**를 선택합니다.

단계 **2** **Export(**내보내기**)**를 선택하고 다음 중 하나를 선택합니다.

- **Export Selected(**선택 항목 내보내기**)**: **Profiling Policies(**프로파일링 정책**)** 창에서 선택한 엔드포인트 프로파일링 정책만 내보낼 수 있습니다.
- **Export Selected with Endpoints(**엔드포인트와 함께 선택한 항목 내보내기**)**: 선택한 엔드포인트 프로파일링 정책 및 해당 정책을 사용하여 프로파일링한 엔드포인트를 내보낼 수 있습니다.
- **Export All(**모두 내보내기**)**: 기본적으로 **Profiling Policies(**프로파일링 정책**)** 창의 모든 프로파일링 정책을 내보낼 수 있습니다.

단계 **3** **OK(**확인**)**를 클릭하여 profiler_policies.xml 파일의 엔드포인트 프로파일링 정책을 내보냅니다.

미리 정의된 엔드포인트 프로파일링 정책

Cisco ISE는 구축될 때 미리 정의된 기본 프로파일링 정책을 포함하며, 계층적 구성에 따라 네트워크에서 식별된 엔드포인트를 분류하고 일치하는 엔드포인트 ID 그룹에 할당할 수 있습니다. 엔드포인트 프로파일링 정책은 계층적이므로 **Profiling Policies(**프로파일링 정책**)** 창에는 디바이스에 대한 일반(상위) 정책 및 Profiling Policies listing(프로파일링 정책 목록) 창에서 상위 정책과 연결된 하위 정책 목록이 표시될 수 있습니다.

Profiling Policies(프로파일링 정책**)** 창에는 엔드포인트 프로파일링 정책과 해당 이름, 유형, 설명 및 상태, 활성화되었는지 여부 또는 검증 대상이 아닌지 여부가 표시됩니다.

엔드포인트 프로파일링 정책 유형은 다음과 같이 분류됩니다.

- Cisco 제공: Cisco ISE에 미리 정의된 엔드포인트 프로파일링 정책은 Cisco 제공 유형으로 식별됩니다.
    - 관리자 수정: 미리 정의된 엔드포인트 프로파일링 정책을 수정하는 경우 엔드포인트 프로파일링 정책은 관리자 수정 유형으로 식별됩니다. Cisco ISE는 업그레이드 과정에서 미리 정의된 엔드포인트 프로파일링 정책에서 변경한 내용을 덮어씁니다.
- 관리자 생성: 관리자가 엔드포인트 프로파일링 정책을 생성하거나 Cisco에서 제공한 엔드포인트 프로파일링 정책을 복제하는 경우 관리자 생성 유형으로 식별됩니다.

하위 정책이 규칙 및 조건을 상속받을 수 있는 일련의 엔드포인트에 대한 일반 정책(상위)을 생성하는 것이 좋습니다. 엔드포인트를 분류해야 하는 경우 엔드포인트를 프로파일링할 때 엔드포인트 프로파일은 먼저 상위 정책과의 일치를 확인한 후 하위 정책과의 일치를 확인해야 합니다.

예를 들어 Cisco-Device는 모든 Cisco 디바이스에 대한 일반 엔드포인트 프로파일링 정책이고 Cisco 디바이스에 대한 다른 정책은 Cisco-Device의 하위 정책입니다. 엔드포인트를 Cisco-IP-Phone 7960으로 분류해야 하는 경우 이 엔드포인트의 엔드포인트 프로파일은 먼저 상위 Cisco-Device 정책과 일치시킨 다음 하위 Cisco-IP-Phone 정책 및 Cisco-IP-Phone 7960 프로파일링 정책 순으로 일치시켜야 보다 효율적인 분류가 가능합니다.

참고 Cisco ISE는 관리자 수정 정책 또는 해당 하위 정책이 여전히 Cisco Provided(Cisco 제공)으로 레이블이 지정되어 있는 경우에도 덮어쓰지 않습니다. 관리자 수정 정책이 삭제되면 이전 Cisco 제공 정책으로 돌아갑니다. 다음에 피드 업데이트가 발생하면 모든 하위 정책이 업데이트됩니다.

업그레이드 중에 덮어쓰기되는 미리 정의된 엔드포인트 프로파일링 정책

프로파일링 정책 페이지에서 기존 엔드포인트 프로파일링 정책을 편집할 수 있습니다. 미리 정의된 엔드포인트 프로파일링 정책을 수정하려면 미리 정의된 엔드포인트 프로파일의 복사본에 모든 컨피그레이션도 저장해야 합니다.

업그레이드 중에 Cisco ISE는 미리 정의된 엔드포인트 프로파일에 저장한 모든 컨피그레이션을 덮어씁니다.

엔드포인트 프로파일링 정책을 삭제할 수 없음

Profiling Policies(프로파일링 정책**)** 창에서 선택한 엔드포인트 프로파일링 정책 또는 모든 엔드포인트 프로파일링 정책을 삭제할 수 있습니다. 기본적으로는 **Profiling Policies(**프로파일링 정책**)** 창에서 모든 엔드포인트 프로파일링 정책을 삭제할 수 있습니다. **Profiling Policies(**프로파일링 정책**)** 창에서 모든 엔드포인트 프로파일링 정책을 선택하여 삭제하려고 할 때 해당 엔드포인트 프로파일링 정책이 다른 엔드포인트 프로파일링 정책이나 권한 부여 정책에 매핑된 경우 이러한 정책 중 일부가 삭제되지 않을 수 있습니다.

- Cisco에서 제공하는 엔드포인트 프로파일링 정책은 삭제할 수 없습니다.
- 엔드포인트 프로파일이 다른 엔드포인트 프로파일의 부모로 정의되어 있으면 **Profiling Policies(**프로파일링 정책**)** 창에서 부모 프로파일을 삭제할 수 없습니다. 예를 들어 Cisco-Device는 Cisco 디바이스에 대한 다른 엔드포인트 프로파일링 정책의 부모 정책입니다.
- 권한 부여 정책에 매핑되어 있는 엔드포인트 프로파일은 삭제할 수 없습니다. 예를 들어 Cisco-IP-Phone은 프로파일링된 Cisco IP 전화 권한 부여 정책에 매핑되어 있으며 Cisco IP 전화에 대한 다른 엔드포인트 프로파일링 정책의 부모 정책입니다.

Draeger 의료 디바이스용 미리 정의된 프로파일링 정책

Cisco ISE에는 Draeger 의료 디바이스용 일반 정책, Draeger-Delta 의료 디바이스용 정책 및 Draeger-M300 의료 디바이스용 정책을 포함하는 기본 엔드포인트 프로파일링 정책이 포함되어 있습니다. Draeger-Delta 및 Draeger-M300 의료 디바이스는 포트 2050 및 2150을 공유하므로 기본 Draeger 엔드포인트 프로파일링 정책을 사용할 때는 이 두 의료 디바이스를 분류할 수 없습니다.

이러한 Draeger 디바이스가 환경에서 포트 2050 및 2150을 공유하는 경우에는 해당 의료 디바이스를 구분할 수 있도록 디바이스 대상 IP 주소 확인을 위한 규칙을 기본 Draeger-Delta 및 Draeger-M300 엔드포인트 프로파일링 정책에 더 추가해야 합니다.

Cisco ISE는 Draeger 의료 디바이스용 엔드포인트 프로파일링 정책에서 사용되는 다음 프로파일링 조건을 포함합니다.

- 포트 2000을 포함하는 Draeger-Delta-PortCheck1
- 포트 2050을 포함하는 Draeger-Delta-PortCheck2
- 포트 2100을 포함하는 Draeger-Delta-PortCheck3
- 포트 2150을 포함하는 Draeger-Delta-PortCheck4
- 포트 1950을 포함하는 Draeger-M300PortCheck1
- 포트 2050을 포함하는 Draeger-M300PortCheck2
- 포트 2150을 포함하는 Draeger-M300PortCheck3

알 수 없는 엔드포인트에 대한 엔드포인트 프로파일링 정책

알 수 없는 엔드포인트는 기존 프로파일과 일치하지 않으며 Cisco ISE에서 프로파일링할 수 없는 엔드포인트입니다. 알 수 없는 프로파일은 엔드포인트에 할당되는 기본 시스템 프로파일링 정책입니다. 이 프로파일에서는 해당 엔드포인트에 대해 수집되는 속성 또는 속성 집합이 Cisco ISE의 기존 프로파일과 일치하지 않습니다.

알 수 없는 프로파일이 할당되는 시나리오는 다음과 같습니다.

- Cisco ISE에서 엔드포인트가 동적으로 검색되었는데 해당 엔드포인트에 일치하는 엔드포인트 프로파일링 정책이 없으면 엔드포인트가 알 수 없는 프로파일에 할당됩니다.
- 엔드포인트가 Cisco ISE에 정적으로 추가되었는데 정적으로 추가된 엔드포인트에 일치하는 엔드포인트 프로파일링 정책이 없으면 엔드포인트가 알 수 없는 프로파일에 할당됩니다.

  네트워크에 엔드포인트를 정적으로 추가한 경우 정적으로 추가된 엔드포인트는 Cisco ISE의 프로파일링 서비스에 의해 프로파일링되지 않습니다. 나중에 알 수 없는 프로파일을 적절한 프로파일로 변경할 수 있으며, Cisco ISE는 할당되었던 프로파일링 정책을 재할당하지 않습니다.

정적으로 추가된 엔드포인트에 대한 엔드포인트 프로파일링 정책

프로파일링 서비스는 정적으로 추가된 엔드포인트를 프로파일링하기 위해 엔드포인트에 새 MATCHEDPROFILE 속성을 추가하여 엔드포인트에 대한 프로파일을 계산합니다. 계산된 프로파일은 엔드포인트가 동적으로 프로파일링되는 경우 해당 엔드포인트의 실제 프로파일입니다. 따라서 정적으로 추가된 엔드포인트에 대해 계산된 프로파일과 동적으로 프로파일링된 엔드포인트의 일치하는 프로파일 간 불일치 여부를 확인할 수 있습니다.

정적 **IP** 디바이스에 대한 엔드포인트 프로파일링 정책

IP 주소가 정적으로 할당된 엔드포인트가 있는 경우 해당 정적 IP 디바이스에 대해 프로파일을 생성할 수 있습니다.

정적 IP 주소를 사용하는 엔드포인트를 프로파일링하려면 RADIUS 프로브나 SNMP 쿼리 및 SNMP 트랩 프로브를 활성화해야 합니다.

엔드포인트 프로파일링 정책 일치

Cisco ISE는 하나 이상의 규칙에 정의되어 있는 프로파일링 조건이 프로파일링 정책에서 충족되면 항상 평가한 정책이 아니라 엔드포인트에 대해 선택한 정책(일치한 정책)을 고려합니다. 여기서 해당 엔드포인트에 대한 정적 할당 상태는 시스템에서 false로 설정됩니다. 그러나 엔드포인트 편집 중에 정적 재할당 기능을 사용하여 시스템의 기존 프로파일링 정책에 엔드포인트를 정적으로 재할당한 후에는 해당 상태를 true로 설정할 수 있습니다.

엔드포인트의 일치한 정책에 적용되는 사항은 다음과 같습니다.

- 정적으로 할당된 엔드포인트의 경우 프로파일링 서비스는 MATCHEDPROFILE을 계산합니다.

- 정적으로 할당된 엔드포인트의 경우에는 MATCHEDPROFILE이 일치하는 엔드포인트 프로파일과 동일합니다.

프로파일링 정책에 정의되어 있는 하나 이상의 규칙을 사용하여 동적 엔드포인트에 일치하는 프로파일링 정책을 확인하고 그룹화를 위해 엔드포인트 ID 그룹을 적절하게 할당할 수 있습니다.

엔드포인트가 기존 정책에 매핑되어 있으면 프로파일링 서비스는 프로파일링 정책의 계층에서 일치하는 정책 그룹을 포함하는 가장 가까운 부모 프로파일을 검색한 다음 엔드포인트를 적절한 엔드포인트 정책에 할당합니다.

권한 부여에 사용되는 엔드포인트 프로파일링 정책

권한 부여 규칙에서 엔드포인트 프로파일링 정책을 사용할 수 있습니다. 이러한 규칙에서는 엔드포인트 프로파일링 정책에 대한 확인을 속성으로 포함하는 새 조건을 생성할 수 있습니다. 해당 속성에는 엔드포인트 프로파일링 정책의 이름이 지정됩니다. PostureApplicable, EndPointPolicy, LogicalProfile 및 BYODRegistration 속성이 포함된 엔드포인트 사전에서 엔드포인트 프로파일링 정책을 선택할 수 있습니다.

PostureApplicable의 속성 값은 운영체제에 따라 자동으로 설정됩니다. AnyConnect 지원은 해당 플랫폼에서 포스처를 수행할 수 없으므로, IOS 및 Android 디바이스에 대해 *No(*아니요*)*로 설정됩니다. 이 값은 Mac OSX 및 Windows 디바이스에 대해서는 *Yes(*예*)*로 설정됩니다.

EndPointPolicy, BYODRegistration 및 ID 그룹 조합을 포함하는 권한 부여 규칙을 정의할 수 있습니다.

논리 프로파일로 그룹화된 엔드포인트 프로파일링 정책

논리 프로파일은 Cisco에서 제공하거나 관리자가 생성한 엔드포인트 프로파일링 정책과는 무관한, 프로파일 범주 또는 연결된 프로파일이 담긴 컨테이너입니다. 엔드포인트 프로파일링 정책은 여러 논리 프로파일에 연결될 수 있습니다.

권한 부여 정책 조건의 논리 프로파일을 사용하여 프로파일 범주에 대한 전반적인 네트워크 액세스 정책을 생성할 수 있습니다. 권한 부여를 위한 단순 조건을 생성할 수 있으며, 이는 권한 부여 규칙에 포함될 수 있습니다. 권한 부여 조건에 사용할 수 있는 속성-값 쌍은 논리 프로파일(속성) 및 논리 프로파일(값)의 이름으로, 이는 엔드포인트 시스템 사전에서 찾을 수 있습니다.

예를 들어 Android, Apple iPhone 또는 Blackberry와 같은 모든 모바일 디바이스에 대한 논리 프로파일을 생성할 수 있는데, 해당 범주의 일치하는 엔드포인트 프로파일링 정책을 논리 프로파일에 할당하면 됩니다. Cisco ISE에는 IP-Phone, Cisco-IP-Phone, Nortel-IP-Phone-2000-Series 및 Avaya-IP-Phone 프로파일 등의 모든 IP Phone의 기본 논리 프로파일인 IP-Phone이 있습니다.

논리적 프로파일 생성

엔드포인트 프로파일링 정책 범주를 그룹화하는 데 사용할 수 있는 논리적 프로파일을 생성할 수 있습니다. 그러면 프로파일 또는 관련 프로파일의 전체 범주를 생성할 수 있습니다. 할당된 집합에서 엔드포인트 프로파일링 정책을 제거하여 사용 가능한 집합으로 다시 이동할 수도 있습니다. 논리적

프로파일에 대한 자세한 내용은 논리 프로파일로 그룹화된 엔드포인트 프로파일링 정책, 244 페이지를 참고하십시오.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Policy(**정책**)** > **Profiling(**프로파일링**)** > **Profiling(**프로파일링**)** > **Logical Profiles(**논리적 프로파일**)**를 선택합니다.

단계 **2** **Add(**추가**)**를 클릭합니다.

단계 **3** **Name(**이름**)** 및 **Description(**설명**)** 텍스트 상자에 새 논리적 프로파일의 이름과 설명을 입력합니다.

단계 **4** **Available Policies(**사용 가능한 정책**)**에서 엔드포인트 프로파일링 정책을 선택하여 논리적 프로파일에 할당합니다.

단계 **5** 오른쪽 화살표를 클릭하여 선택한 엔드포인트 프로파일링 정책을 **Assigned Policies(**할당된 정책**)**로 이동합니다.

단계 **6** **Submit(**제출**)**을 클릭합니다.

프로파일링 예외 작업

예외 작업은 엔드포인트 프로파일링에서 참조될 수 있으며 작업과 연결된 예외 조건이 충족되는 경우 트리거되는 단일의 구성 가능한 작업입니다.

예외 작업은 다음 유형 중 하나일 수 있습니다.

- Cisco 제공 - Cisco 제공 예외 작업은 삭제할 수 없습니다. Cisco ISE에서 엔드포인트를 프로파일링하려는 경우 Cisco ISE는 시스템에서 다음과 같은 편집 불가능한 프로파일링 예외 작업을 트리거합니다.
  - 권한 부여 변경 - 권한 부여 정책에 사용되는 엔드포인트 ID 그룹에서 엔드포인트가 추가되거나 제거될 때 프로파일링 서비스는 CoA(Change of Authorization)를 실행합니다.
  - 엔드포인트 삭제 - 엔드포인트가 시스템의 엔드포인트 페이지에서 삭제되거나 Cisco ISE 네트워크의 편집 페이지에서 알 수 없는 프로파일로 다시 할당되면, Cisco ISE에서 예외 작업이 트리거되고 CoA가 실행됩니다.
  - FirstTimeProfiled - 엔드포인트가 Cisco ISE에서 처음 프로파일링되는 경우 Cisco ISE에서 예외 작업이 트리거되고 CoA가 실행됩니다. 이 경우 엔드포인트의 프로파일이 알 수 없는 프로파일에서 기존 프로파일로 변경되지만 Cisco ISE 네트워크에서 엔드포인트가 성공적으로 인증되지 않습니다.
- 관리자 생성 - Cisco ISE에서 관리자가 생성한 프로파일링 예외 작업을 트리거합니다.

예외 작업 생성

하나 이상의 예외 규칙을 정의하여 단일 프로파일링 정책에 연결할 수 있습니다. 이와 같이 연결하는 경우 프로파일링 정책이 일치하며 Cisco ISE의 프로파일링 엔드포인트에서 하나 이상의 예외 규칙이 일치하면 예외 작업(구성 가능한 단일 작업)이 트리거됩니다.

단계 1 Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Policy(**정책**)** > **Policy Elements(**정책 요소**)** > **Results(**결과**)** > **Profiling(**프로파일링**)** > **Exception Actions(**예외 작업**)**를 선택합니다.

단계 2 **Add(**추가**)**를 클릭합니다.

단계 3 **Name(**이름**)** 및 **Description(**설명**)** 텍스트 상자에 예외 작업의 이름과 설명을 입력합니다.

단계 4 **CoA Action(CoA** 작업**)** 확인란을 선택합니다.

단계 5 **Policy Assignment(**정책 할당**)** 드롭다운 목록을 클릭하고 엔드포인트 정책을 선택합니다.

단계 6 **Submit(**제출**)**을 클릭합니다.

정책 및 ID 그룹을 정적으로 할당하여 엔드포인트 생성

엔드포인트 페이지에서 엔드포인트의 MAC 주소를 사용하여 새 엔드포인트를 정적으로 생성할 수 있습니다. 또한 엔드포인트 페이지에서 정적 할당용으로 엔드포인트 프로파일링 정책 및 ID 그룹을 선택할 수도 있습니다.

엔드포인트 ID 목록에는 일반 및 모바일 디바이스(MDM) 엔드포인트가 표시됩니다. 목록 페이지에는 MDM 엔드포인트에 대한 호스트 이름, 디바이스 유형, 디바이스 식별자 등의 속성에 해당하는 열이 표시됩니다. 정적 할당, 정적 그룹 할당 등의 기타 열은 기본적으로 표시되지 않습니다.

참고 이 페이지를 사용하여 MDM 엔드포인트 추가, 편집, 삭제, 가져오기 또는 내보내기를 수행할 수는 없습니다.

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

단계 2 **Add(**추가**)**를 클릭합니다.

단계 3 엔드포인트의 MAC 주소를 쉼표로 구분된 16진수 형식으로 입력합니다.

단계 4 **Policy Assignment(**정책 할당**)** 드롭다운 목록에서 일치하는 엔드포인트 정책을 선택하여 정적 할당 상태를 동적에서 정적으로 변경합니다.

단계 5 **Static Assignment(**정적 할당**)** 확인란을 선택하여 엔드포인트에 할당되어 있는 정적 할당 상태를 동적에서 정적으로 변경합니다.

단계 6 **Identity Group Assignment(ID** 그룹 할당**)** 드롭다운 목록에서 새로 생성하는 엔드포인트를 할당할 엔드포인트 ID 그룹을 선택합니다.

단계 7 **Static Group Assignment(**정적 그룹 할당**)** 확인란을 선택하여 엔드포인트 ID 그룹의 동적 할당을 정적으로 변경합니다.

단계 8 **Submit(**제출**)**을 클릭합니다.

CSV 파일에서 엔드포인트 가져오기

Cisco ISE 템플릿에서 생성한 CSV 파일에서 엔드포인트를 가져와 엔드포인트 세부정보로 업데이트할 수 있습니다. ISE에서 내보낸 엔드포인트는 약 75개의 속성을 포함하므로, 다른 ISE 구축으로 직접 가져올 수 없습니다. 가져올 수 없는 열이 CSV 파일에 있으면 열 목록이 포함된 메시지가 표시됩니다. 파일을 다시 가져오기 전에 지정된 열을 삭제해야 합니다.

참고 엔드포인트 사용자 맞춤화 속성을 가져오려면 올바른 데이터 유형을 사용하여 **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **Settings(**설정**)** > **Endpoint Custom Attributes(**엔드포인트 사용자 맞춤화 속성**)** 페이지의 CSV 파일에서와 동일한 사용자 맞춤화 속성을 만들어야합니다. 이러한 속성은 "CUSTOM."으로 시작되어 엔드포인트 속성과 차별화되어야 합니다.

가져올 수 있는 속성은 약 30개입니다. 목록에는 MACAddress, EndPointPolicy 및 IdentityGroup이 포함됩니다. 선택할 수 있는 속성은 다음과 같습니다.

설명	PortalUser	LastName
PortalUser.GuestType	PortalUser.FirstName	EmailAddress
PortalUser.Location	Device Type	host-name
PortalUser.GuestStatus	StaticAssignment	Location
PortalUser.CreationType	StaticGroupAssignment	MDMEnrolled
PortalUser.EmailAddress	User-Name	MDMOSVersion
PortalUser.PhoneNumber	DeviceRegistrationStatus	MDMServerName
PortalUser.LastName	AUPAccepted	MDMServerID
PortalUser.GuestSponsor	FirstName	BYODRegistration
CUSTOM.<custom attribute name>	—	—

엔드포인트 목록이 MACAddress, EndpointPolicy, IdentityGroup <위에서 선택적 속성으로 나열된 속성 목록> 순으로 나타나도록 파일 헤더는 기본 가져오기 템플릿에 지정된 형식이어야 합니다. 다음 파일 템플릿을 생성할 수 있습니다.

- MACAddress
- MACAddress, EndPointPolicy
- MACAddress, EndPointPolicy, IdentityGroup
- MACAddress, EndPointPolicy, IdentityGroup, <위에서 선택적 속성으로 나열된 속성 목록>

CSV 파일에서 엔드포인트를 가져오는 경우 MAC 주소를 제외한 모든 속성 값은 선택 사항입니다. 특정 값 없이 엔드포인트를 가져오려는 경우 값을 쉼표로 구분합니다. 예를 들면 다음과 같습니다.

- MAC1, Endpoint Policy1, Endpoint Identity Group1
- MAC2
- MAC3, Endpoint Policy3
- MAC4, Endpoint Identity Group4
- MAC5, , Endpoint Identity Group5, MyDescription, MyPortalUser 등

단계 **1** **Context Visibility(**상황 가시성**)** > **Endpoints(**엔드포인트**)** > **Import(**가져오기**)** 를 선택합니다.
단계 **2** **Import From File(**파일에서 가져오기**)**을 클릭합니다.
단계 **3** **Browse(**찾아보기**)**를 클릭하여 이미 생성한 CSV 파일을 찾습니다.
단계 **4** **Submit(**제출**)**을 클릭합니다.

엔드포인트에 사용할 수 있는 기본 가져오기 템플릿

엔드포인트를 가져오는 데 사용할 수 있는 템플릿을 생성하여 엔드포인트를 업데이트할 수 있습니다. 기본적으로, Generate a Template(템플릿 생성) 링크를 사용하여 Microsoft Office Excel 애플리케이션에서 CSV 파일을 생성하고 파일을 로컬로 시스템에 저장할 수 있습니다. 파일은 **Context Visibility(**상황 가시성**)** > **Endpoints(**엔드포인트**)** > **Import(**가져오기**)** > **Import From File(**파일에서 가져오기**)**에서 찾을 수 있습니다. Generate a Template(템플릿 생성) 링크를 사용하여 템플릿을 생성하면 Cisco ISE 서버에 Opening template.csv(template.csv 여는 중) 대화 상자가 표시됩니다. 이 대화 상자를 사용하면 기본 template.csv 파일을 열거나, template.csv 파일을 로컬로 시스템에 저장할 수 있습니다. 대화 상자에서 template.csv 파일 열기를 선택하는 경우 파일이 Microsoft Office Excel 애플리케이션에서 열립니다. 기본 template.csv 파일에는 MAC 주소, 엔드포인트 정책 및 엔드포인트 ID, 그리고 기타 선택 속성을 표시하는 헤더 행이 포함되어 있습니다.

엔드포인트의 MAC 주소, 엔드포인트 프로파일링 정책 및 엔드포인트 ID 그룹 그리고 가져오고자 하는 선택 속성값을 업데이트하고, 이를 새로운 파일명으로 저장합니다. 이 파일은 엔드포인트를 가져오는 데 사용할 수 있습니다. Generate a Template(템플릿 생성) 링크를 사용하는 경우 작성된 template.csv 파일의 헤더 행을 참고해 주십시오.

표 ***56: CSV*** 템플릿 파일

MAC	**EndPointPolicy**	**IdentityGroup**	기타 선택 속성
11:11:11:11:11:11	Android	Profiled	<Empty>/<Value>

가져오기 중에 알 수 없는 엔드포인트가 다시 프로파일링됨

가져오기에 사용되는 파일에 포함된 엔드포인트에 MAC 주소가 있으며 이러한 엔드포인트에 할당된 엔드포인트 프로파일링 정책이 알 수 없음 프로파일인 경우 해당 엔드포인트는 가져오기 중에 Cisco ISE에서 일치하는 엔드포인트 프로파일링 정책으로 즉시 다시 프로파일링됩니다. 그러나 알 수 없음 프로파일에 정적으로 할당되지는 않습니다. CSV 파일에서 엔드포인트 프로파일링 정책이 할당되어 있지 않은 엔드포인트는 알 수 없음 프로파일에 할당된 다음 일치하는 엔드포인트 프로파

일링 정책으로 다시 프로파일링됩니다. 다음 표에는 Cisco ISE가 가져오기 중에 Xerox_Device 프로파일과 일치하는 알 수 없음 프로파일을 다시 프로파일링하고 할당되지 않은 엔드포인트를 다시 프로파일링하는 방법이 나와 있습니다.

표 ***57:*** 알 수 없음 프로파일*:* 파일에서 가져오기

MAC 주소	**Cisco ISE**에서 가져오기 전에 할당된 엔드포인트 프로파일링 정책	**Cisco ISE**에서 가져오기 후에 할당되는 엔드포인트 프로파일링 정책
00:00:00:00:01:02	Unknown(알 수 없음)	Xerox-Device
00:00:00:00:01:03	Unknown(알 수 없음)	Xerox-Device
00:00:00:00:01:04	Unknown(알 수 없음)	Xerox-Device
00:00:00:00:01:05	프로파일이 할당되어 있지 않은 엔드포인트는 알 수 없음 프로파일로 할당되는 동시에 일치하는 프로파일로 다시 프로파일링됩니다.	Xerox-Device

잘못된 속성을 포함하는 엔드포인트를 가져올 수 없음

CSV 파일에 있는 엔드포인트 중 하나에 잘못된 속성이 있는 경우 엔드포인트를 가져올 수 없으며 오류 메시지가 표시됩니다.

예를 들어 가져오기에 사용하는 파일에서 엔드포인트가 잘못된 프로파일에 할당되어 있으면 Cisco ISE에 일치하는 프로파일이 없으므로 가져올 수 없습니다. CSV 파일에서 잘못된 프로파일에 할당된 엔드포인트가 가져오기되지 않는 방식은 아래 표를 참고해 주십시오.

표 ***58:*** 잘못된 프로파일*:* 파일에서 가져오기

MAC 주소	**Cisco ISE**에서 가져오기 전에 할당된 엔드포인트 프로파일링 정책	**Cisco ISE**에서 가져오기 후에 할당되는 엔드포인트 프로파일링 정책
00:00:00:00:01:02	Unknown(알 수 없음)	Xerox-Device
00:00:00:00:01:05	00:00:00:00:01:05 등의 엔드포인트가 Cisco ISE에서 사용 가능한 프로파일이 아닌 잘못된 프로파일에 할당되어 있으면 Cisco ISE에는 정책 이름이 잘못되었으며 엔드포인트를 가져오지 않는다는 경고 메시지가 표시됩니다.	Cisco ISE에 일치하는 프로파일이 없으므로 엔드포인트를 가져오지 않습니다.

LDAP 서버에서 엔드포인트 가져오기

LDAP 서버에서 엔드포인트의 MAC 주소, 연결된 프로파일 및 엔드포인트 ID 그룹을 안전하게 가져올 수 있습니다.

시작하기 전에

엔드포인트 가져오기를 시작하기 전에 LDAP 서버에 다음 항목을 설치했는지 확인합니다.

연결 설정 및 쿼리 설정을 구성해야 LDAP 서버에서 가져오기를 수행할 수 있습니다. Cisco ISE에서 연결 설정 또는 쿼리 설정이 잘못 구성되어 있으면 "LDAP 가져오기 실패:" 오류 메시지가 표시됩니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Context Visibility(**상황 가시성**)** > **Endpoints(**엔드포인트 > **Import(**가져오기**)** > **Import from LDAP(LDAP**에서 가져오기**)**를 선택합니다.

단계 **2** 연결 설정에 대한 값을 입력합니다.

단계 **3** 쿼리 설정에 대한 값을 입력합니다.

단계 **4** **Submit(**제출**)**을 클릭합니다.

쉼표로 구분된 값을 사용하여 엔드포인트 내보내기

Cisco ISE 서버에서 선택한 엔드포인트 또는 모든 엔드포인트를 CSV 파일로 내보낼 수 있습니다. 이 파일에서는 엔드포인트와 약75개 속성이 해당 MAC 주소, 엔드포인트 프로파일링 정책 및 엔드포인트 ID 그룹과 함께 나열됩니다. Cisco ISE에서 생성된 사용자 맞춤화 속성도 CSV 파일로 내보내지며 다른 엔드포인트 속성과 구별할 수 있도록 "CUSTOM"이라는 접두사가 붙습니다.

참고 한 구축에서 다른 구축으로 내보낸 엔드포인트 사용자 맞춤화 속성을 가져오려면 **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **Settings(**설정**)** > **Endpoint Custom Attributes(**엔드포인트 사용자 맞춤화 속성**)** 창에서 동일한 사용자 맞춤화 속성을 생성하고 원래 구축에 지정된 것과 동일한 데이터 유형을 사용해야 합니다.

Export All(모두 내보내기**)**은 Cisco ISE의 모든 엔드 포인트를 내보내는 반면 **Export Selected(**선택 항목 내보내기**)**는 사용자가 선택한 엔드포인트만 내보냅니다. 기본적으로 profiler_endpoints.csv는 CSV 파일이고 CSV 파일을 여는 기본 애플리케이션은 Microsoft Office Excel입니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Context Visibility(**상황 가시성**)** > **Endpoints(**엔드포인트**)**를 선택합니다.

단계 **2** **Export(**내보내기**)**를 클릭하고 다음 중 하나를 선택합니다.

- **Export Selected(**선택 항목 내보내기**)**: 엔드포인트 창에서 선택한 엔드포인트만 내보낼 수 있습니다.
- **Export All(**모두 내보내기**)**: 기본적으로 엔드포인트 창의 모든 프로파일링 엔드포인트를 내보낼 수 있습니다.

단계 **3** **OK(**확인**)**를 클릭하여 profiler_endpoints.csv 파일을 저장합니다.

식별된 엔드포인트

Cisco ISE는 네트워크에 연결하고 네트워크의 리소스를 사용하는 것으로 식별된 엔드포인트를 엔드포인트 페이지에 표시합니다. 엔드포인트는 일반적으로 유선/무선 네트워크 액세스 디바이스 및 VPN을 통해 네트워크에 연결되는 네트워크 지원 디바이스입니다. 엔드포인트는 개인용 컴퓨터, 랩탑, IP Phone, 스마트폰, 게임 콘솔, 프린터, 팩스 기기 등이 될 수 있습니다.

16진수 형식으로 표시되는 엔드포인트의 MAC 주소는 항상 고유한 엔드포인트 표시이지만, 다양한 속성 집합과 그에 연결된 값(속성-값 쌍이라고 함)으로 엔드포인트를 식별할 수 있습니다. 엔드포인트 기능, 네트워크 액세스 디바이스의 기능과 컨피그레이션, 그리고 이러한 속성을 수집하는 데 사용하는 방법(프로브)에 따라 엔드포인트에 대한 다양한 속성 집합을 수집할 수 있습니다.

동적으로 프로파일링된 엔드포인트

네트워크에서 검색된 엔드포인트는 구성된 프로파일링 엔드포인트 프로파일링 정책을 기준으로 동적으로 프로파일링될 수 있으며, 해당 프로파일에 따라 일치하는 엔드포인트 ID 그룹에 할당될 수 있습니다.

정적으로 프로파일링된 엔드포인트

MAC 주소를 사용하여 엔드포인트를 생성하고 Cisco ISE에서 엔드포인트 ID 그룹과 함께 프로파일을 연결하면 엔드포인트를 정적으로 프로파일링할 수 있습니다. Cisco ISE는 정적으로 할당된 엔드포인트에 대해 프로파일링 정책 및 ID 그룹을 다시 할당하지 않습니다.

알 수 없는 엔드포인트

엔드포인트에 대해 일치하는 프로파일링 정책이 없으면 알 수 없는 프로파일링 정책(알 수 없음)을 할당할 수 있으며 엔드포인트는 그에 따라 알 수 없음으로 프로파일링됩니다. 알 수 없음 엔드포인트 정책으로 프로파일링된 엔드포인트의 경우 해당 엔드포인트에 대해 수집된 속성 또는 속성 집합을 사용하여 프로파일을 생성해야 합니다. 프로파일과 일치하지 않는 엔드포인트는 알 수 없음 엔드포인트 ID 그룹 내에서 그룹화됩니다.

정책 서비스 노드 데이터베이스에 로컬로 저장되는 식별된 엔드포인트

Cisco ISE는 식별된 엔드포인트를 정책 서비스 노드 데이터베이스에 로컬로 씁니다. 데이터베이스에 로컬로 저장된 이러한 엔드포인트는 엔드포인트에서 중요한 속성이 변경되는 경우에만 관리 노드 데이터베이스에서 사용할 수 있으며(원격 쓰기) 다른 정책 서비스 노드 데이터베이스로 복제됩니다.

중요한 속성은 다음과 같습니다.

- ip
- EndPointPolicy

- MatchedValue
- StaticAssignment
- StaticGroupAssignment
- MatchedPolicyID
- NmapSubnetScanID
- PortalUser
- DeviceRegistrationStatus
- BYODRegistration

Cisco ISE에서 엔드포인트 프로파일정의를 변경할 때는 모든 엔드포인트를 다시 프로파일링해야 합니다. 엔드포인트의 속성을 수집하는 정책 서비스 노드가 해당 엔드포인트를 다시 프로파일링합니다.

다른 정책 서비스 노드에서 속성이 처음 수집된 엔드포인트에 대해 정책 서비스 노드가 속성 수집을 시작하면 엔드포인트 소유권이 현재 서비스 노드로 변경됩니다. 새 정책 서비스 노드는 이전 정책 서비스 노드에서 최신 속성을 검색하며, 수집한 속성을 이미 수집된 속성에 따라 조정합니다.

엔드포인트에서 중요한 속성이 변경되면 해당 엔드포인트의 속성이 관리 노드 데이터베이스에 자동으로 저장되므로 엔드포인트에 최신 중요 변경사항이 적용됩니다. 엔드포인트를 소유하는 정책 서비스 노드를 사용할 수 없는 경우에는 소유자가 없어진 엔드포인트를 관리자 ISE 노드가 다시 프로파일링하며, 해당 엔드포인트에 대해 새 정책 서비스 노드를 구성해야 합니다.

클러스터의 정책 서비스 노드

Cisco ISE는 정책 서비스 노드 그룹을 클러스터로 사용합니다. 이를 통해 클러스터에서 둘 이상의 노드가 동일 엔드포인트에 대한 속성을 수집할 때 엔드포인트 속성을 교환할 수 있습니다. 로드 밸런서 뒤에 있는 모든 정책 서비스 노드에 대해 클러스터를 생성하는 것이 좋습니다.

현재 소유자와 다른 노드가 동일 엔드포인트에 대한 속성을 수신하는 경우, 해당 노드는 속성을 병합하고 소유권을 변경해야 하는지를 확인하기 위해 현재 소유자로부터 최신 속성을 요청하는 메시지를 클러스터를 통해 전송합니다. Cisco ISE에서 노드 그룹을 정의하지 않은 경우에는 모든 노드가 하나의 클러스터 내에 있다고 가정합니다.

Cisco ISE에서 수행되는 엔드포인트 생성 및 복제는 변경되지 않습니다. 즉, 정적 속성과 동적 속성에서 구축되는 프로파일링에 사용되는 속성의 허용 목록을 기준으로 엔드포인트에 대한 소유권 변경 여부만 결정합니다.

후속 속성 수집 시 다음 속성이 변경되면 관리 노드에서 엔드포인트가 업데이트됩니다.

- ip
- EndPointPolicy
- MatchedValue
- StaticAssignment

- StaticGroupAssignment
- MatchedPolicyID
- NmapSubnetScanID
- PortalUser
- DeviceRegistrationStatus
- BYODRegistration

엔드포인트를 편집하여 관리 노드에 저장하면 엔드포인트의 현재 소유자에서 속성을 검색합니다.

엔드포인트 ID 그룹 생성

Cisco ISE는 검색되는 엔드포인트를 해당하는 엔드포인트 ID 그룹으로 그룹화합니다. Cisco ISE에서는 몇 가지 시스템 정의 엔드포인트 ID 그룹이 제공됩니다. 엔드포인트 **ID** 그룹 창에서 엔드포인트 ID 그룹을 추가로 생성할 수도 있습니다. 직접 생성한 엔드포인트 ID 그룹은 편집하거나 삭제할 수 있습니다. 시스템 정의 엔드포인트 ID 그룹의 경우 설명만 편집할 수 있습니다. 그 이름은 편집하거나 삭제할 수 없습니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **Groups(**그룹**)** > **Endpoint Identity Groups(**엔드포인트 **ID** 그룹**)**를 선택합니다.

단계 **2** **Add(**추가**)**를 클릭합니다.

단계 **3** 생성할 엔드포인트 ID 그룹의 **Name(**이름**)**을 입력합니다(엔드포인트 ID 그룹의 이름에 공백 제외).

단계 **4** 생성할 엔드포인트 ID 그룹에 대한 **Description(**설명**)**을 입력합니다.

단계 **5** **Parent Group(**부모 그룹**)** 드롭다운 목록을 클릭하여 새로 생성한 엔드포인트 ID 그룹을 연결할 엔드포인트 ID 그룹을 선택합니다.

단계 **6** **Submit(**제출**)**을 클릭합니다.

엔드포인트 ID 그룹에서 그룹화되어 식별된 엔드포인트

Cisco ISE는 엔드포인트 프로파일링 정책에 따라 검색된 엔드포인트를 해당하는 엔드포인트 ID 그룹으로 그룹화합니다. 프로파일링 정책은 계층적이며 Cisco ISE의 엔드포인트 식별 그룹 수준에서 적용됩니다. 엔드포인트를 엔드포인트 ID 그룹으로 그룹화하고 프로파일링 정책을 엔드포인트 ID 그룹에 적용하면, 해당 엔드포인트 프로파일링 정책을 검사하여 Cisco ISE에서 엔드포인트와 엔드포인트 프로파일의 매핑을 확인할 수 있습니다.

Cisco ISE는 기본적으로 일련의 엔드포인트 ID 그룹을 생성하며, 관리자는 엔드포인트가 동적으로 또는 정적으로 할당될 수 있는 고유한 ID 그룹을 생성할 수 있습니다. 엔드포인트 ID 그룹을 생성하고 ID 그룹을 시스템에서 생성된 ID 그룹 중 하나와 연결할 수 있습니다. 또한 생성한 엔드포인트를

시스템에 존재하는 ID 그룹 중 하나에 정적으로 할당할 수 있으며, 프로파일링 서비스는 ID 그룹을 다시 할당할 수 없습니다.

엔드포인트에 대해 생성된 기본 엔드포인트 ID 그룹

Cisco ISE에서는 다음과 같은 엔드포인트 ID 그룹을 생성합니다.

- Blocked List: 이 엔드포인트 ID 그룹에는 Cisco ISE의 이 그룹에 정적으로 할당된 엔드포인트 및 디바이스 등록 포털에서 차단된 엔드포인트가 포함됩니다. Cisco ISE에서 이 그룹의 엔드포인트에 대한 네트워크 액세스를 허용하거나 거부하도록 권한 부여 프로파일을 정의할 수 있습니다.
- GuestEndpoints: 이 엔드포인트 ID 그룹에는 게스트 사용자가 사용하는 엔드포인트가 포함됩니다.
- Profiled: 이 엔드포인트 ID 그룹에는 Cisco IP 전화기 및 Cisco ISE의 워크스테이션을 제외하고 엔드포인트 프로파일링 정책과 일치하는 엔드포인트가 포함됩니다.
- RegisteredDevices: 이 엔드포인트 ID 그룹에는 직원이 디바이스 등록 포털을 통해 추가한 등록된 디바이스에 해당하는 엔드포인트가 포함됩니다. 프로파일링 서비스는 이 그룹에 할당된 디바이스를 정상적으로 프로파일링합니다. 엔드포인트는 Cisco ISE의 이 그룹에 정적으로 할당되며, 프로파일링 서비스는 해당 엔드포인트를 다른 ID 그룹에 다시 할당할 수 없습니다. 이러한 디바이스는 다른 엔드포인트와 마찬가지로 엔드포인트 목록에 표시됩니다. 디바이스 등록 포털을 통해 Cisco ISE의 Endpoints(엔드포인트) 창에 있는 엔드포인트 목록에서 추가한 디바이스는 편집, 삭제 및 차단할 수 있습니다. 디바이스 등록 포털에서 차단된 디바이스는 Blocked List 엔드포인트 ID 그룹에 할당되고, Cisco ISE에 있는 권한 부여 프로파일은 차단된 디바이스를 "Unauthorised Network Access(무단 네트워크 액세스)"라고 표시된 URL로 리디렉션합니다. 이는 차단된 디바이스에 대한 기본 포털 페이지입니다.
- Unknown: 이 엔드포인트 ID 그룹에는 Cisco ISE의 프로파일과 일치하지 않는 엔드포인트가 포함됩니다.

시스템에서 생성된 위의 엔드포인트 ID 그룹 외에 Cisco ISE에서는 프로파일링된(부모) ID 그룹에 연결되는 다음 엔드포인트 ID 그룹도 생성합니다. 부모 그룹이란 시스템에 있는 기본 ID 그룹을 의미합니다.

- Cisco-IP-Phone: 네트워크에서 프로파일링된 모든 Cisco IP 전화기가 포함된 ID 그룹입니다.
- Workstation: 네트워크에서 프로파일링된 모든 워크스테이션이 포함된 ID 그룹입니다.

일치하는 엔드포인트 프로파일링 정책에 대해 생성된 엔드포인트 ID 그룹

기존 정책과 일치하는 엔드포인트 정책이 있는 경우 프로파일링 서비스는 일치하는 엔드포인트 ID 그룹을 생성할 수 있습니다. 이 ID 그룹은 프로파일링된 엔드포인트 ID 그룹의 하위 그룹이 됩니다. 엔드포인트 정책을 생성할 때 프로파일링 정책 페이지에서 Create Matching Identity Group(일치하는 ID 그룹 생성) 확인란을 선택하여 일치하는 엔드포인트 ID 그룹을 생성할 수 있습니다. 프로파일 매핑을 제거하지 않는 한 일치하는 ID 그룹은 삭제할 수 없습니다.

엔드포인트 ID 그룹에서 정적 엔드포인트 추가

엔드포인트 ID 그룹에서 엔드포인트를 추가하거나 정적으로 추가된 엔드포인트를 제거할 수 있습니다.

엔드포인트 위젯의 엔드포인트는 특정 ID 그룹에만 추가할 수 있습니다. 특정 엔드포인트 ID 그룹에 추가하는 엔드포인트는 이전에 동적으로 그룹화되었던 엔드포인트 ID 그룹에서 이동됩니다.

엔드포인트를 최근 추가했던 엔드포인트 ID 그룹에서 제거하는 경우 해당하는 ID 그룹으로 다시 프로파일링됩니다. 엔드포인트는 시스템에서 삭제되지는 않으며 엔드포인트 ID 그룹에서만 제거됩니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **Identity Management(ID** 관리**)** > **Groups(**그룹**)** > **Endpoint Identity Groups(**엔드포인트 **ID** 그룹**)**를 선택합니다.

단계 **2** 엔드포인트 ID 그룹을 선택하고 **Edit(**편집**)**를 클릭합니다.

단계 **3** **Add(**추가**)**를 클릭합니다.

단계 **4** 엔드포인트 위젯에서 엔드포인트를 선택하여 엔드포인트 ID 그룹에 추가합니다.

단계 **5** 엔드포인트 ID 그룹 페이지로 돌아가려면 **Endpoint Group List(**엔드포인트 그룹 목록**)** 링크를 클릭합니다.

ID 그룹에서 추가 또는 제거된 후에 다시 프로파일링되는 동적 엔드포인트

엔드포인트 ID 그룹 할당이 정적이 아닌 경우 엔드포인트 ID 그룹에서 추가하거나 제거한 엔드포인트는 다시 프로파일링됩니다. ISE 프로파일러에서 동적으로 식별되는 엔드포인트는 적절한 엔드포인트 ID 그룹에 표시됩니다. 엔드포인트 ID 그룹에서 동적으로 추가된 엔드포인트를 제거하면 Cisco ISE에서 엔드포인트를 ID 그룹에서 성공적으로 제거했지만 엔드포인트 ID 그룹에서 다시 프로파일링된다는 메시지가 표시됩니다.

권한 부여 규칙에 사용되는 엔드포인트 ID 그룹

권한 부여 정책에서 엔드포인트 ID 그룹을 효율적으로 사용하면 검색된 엔드포인트에 대해 적절한 네트워크 액세스 권한을 제공할 수 있습니다. 예를 들어 모든 유형의 Cisco IP Phone에 대한 권한 부여 규칙은 기본적으로 Cisco ISE의 **Policy(**정책**)** > **Policy Sets(**정책 집합**)** > **Default(**기본값**)** > **Authorization Policy(**권한 부여 정책**)** 위치에서 사용 가능합니다.

엔드포인트 프로파일링 정책이 독립형 정책(다른 엔드포인트 프로파일링 정책의 부모 정책이 아님)인지 아니면 엔드포인트 프로파일링 정책의 부모 정책이 비활성화되어 있지 않은지를 확인해야 합니다.

Anycast 및 프로파일러 서비스

Anycast는 동일한 IP 주소가 둘 이상의 호스트에 할당되고 라우팅을 통해 데이터 수신에 가장 적합한 대상을 결정할 수 있는 네트워킹 기술입니다. 프로파일링 데이터(RADIUS, DHCP 릴레이, SNMP 트랩, NetFlow)에 대한 단일 대상을 제공하기 위한 로드 밸런서 활용 사례와 유사하게, Anycast에서는 여러 대상에 동일한 데이터를 전송하지 않도록 소스에 단일 IP 대상을 구성할 수 있습니다.

Anycast IP 주소는 데이터 센터 간의 리던던시(redundancy)를 지원하기 위해 실제 PSN 인터페이스 IP 주소 또는로드 밸런서 가상 IP 주소에 할당할 수 있습니다. Anycast IP 주소를 ISE 기가비트 이더넷 0 관리 인터페이스에 할당해서는 안됩니다.

Anycast에 사용되는 인터페이스는 프로파일러 프로브에서 사용하는 전용 인터페이스여야 합니다. Anycast IP 주소가 로드 밸런서 가상 IP 주소에 할당된 경우 동일한 요구 사항이 적용되지 않습니다.

Anycast를 사용할 때는 노드 장애를 자동으로 탐지하고 장애가 발생한 노드에 대한 해당 경로를 라우팅 표에서 제거해야 합니다. Anycast 대상이 링크 또는 VLAN의 유일한 호스트인 경우 장애가 발생하면 경로가 자동으로 제거될 수 있습니다.

IP Anycast를 구축할 때는 각 대상에 대한 경로 메트릭이 큰 가중치 또는 바이어스를 갖도록 해야 합니다. Anycast 대상에 대한 경로가 플랩되거나 ECMP(Equal-Cost Multi-Path Routing) 시나리오가 발생하는 경우, 지정된 서비스(RADIUS AAA, DHCP 또는 SNMP 트랩 프로파일링, HTTPS 포털)에 대한 트래픽이 각 대상에 분산되어 과도한 트래픽 및 서비스 장애(RADIUS AAA 및 HTTPS 포털)가 발생하거나 프로파일링 및 데이터베이스 복제(프로파일링 서비스)가 최적화되지 않을 수 있습니다.

IP Anycast의 주요 이점은 액세스 디바이스, 프로파일 데이터 소스 및 DNS의 구성을 크게 간소화한다는 것입니다. 또한 지정된 엔드포인트의 데이터가 단일 PSN으로만 전송되도록 하여 ISE 프로파일링을 최적화할 수 있습니다. 추가 경로 구성을 신중하게 계획하고 적절한 모니터링을 통해 관리해야 합니다. 그러나 고유한 서브 네트워크 및 IP 주소가 사용되지 않으므로 문제 해결이 어려울 수 있습니다.

프로파일러 피드 서비스

프로파일러 조건, 예외 작업 및 NMAP 스캔 작업은 Cisco 제공 항목 또는 관리자 생성 항목으로 분류됩니다(시스템 유형 속성 참고). 또한 엔드포인트 프로파일링 정책은 Cisco 제공, 관리자 생성 또는 관리자 수정 정책으로 분류됩니다. 이러한 분류는 System Type(시스템 유형) 속성에 표시됩니다.

시스템 유형 속성에 따라 프로파일러 조건, 예외 작업, NMAP 스캔 작업 및 엔드포인트 프로파일링 정책에 대해 각기 다른 작업을 수행할 수 있습니다. Cisco 제공 조건, 예외 작업 및 NMAP 스캔 작업은 편집하거나 삭제할 수 없습니다. Cisco에서 제공하는 엔드포인트 정책은 삭제할 수 없습니다. 정책을 편집할 경우 이를 관리자 수정이라고 합니다. 피드 서비스가 정책을 업데이트하면 관리자 수정 정책이 해당 정책 기반으로 하는 최신 버전의 Cisco 제공 정책으로 대체됩니다.

Cisco 피드 서버에서 신규 및 업데이트된 엔드포인트 프로파일링 정책과 MAC OUI 데이터베이스 업데이트를 검색할 수 있습니다. Cisco ISE를 구독하고 있어야 합니다. 적용된, 성공 및 실패 메시지에 대한 이메일 알림을 받을 수도 있습니다. 피드 서비스 작업에 대한 익명 정보를 Cisco에 다시 보낼 수 있습니다. 그러면 Cisco가 피드 서비스를 개선하는 데 도움이 됩니다.

OUI 데이터베이스에는 벤더에게 할당된 MAC OUI가 포함되어 있습니다. OUI 목록은 여기에서 확인할 수 있습니다. http://standards.ieee.org/develop/regauth/oui/oui.txt

Cisco ISE는 정책 및 OUI 데이터베이스 업데이트를 현지 Cisco ISE 서버 표준 시간대를 기준으로 매일 오전 1시에 다운로드합니다. Cisco ISE는 이 다운로드된 피드 서버 정책을 자동으로 적용하며 이러한 변경 사항을 이전 상태로 되돌릴 수 있도록 변경 사항 집합을 저장합니다. 마지막으로 적용한 변경 사항을 되돌리면 새로 추가된 엔드포인트 프로파일링 정책이 제거되고 업데이트된 엔드포인트 프로파일링 정책도 이전 상태로 되돌려집니다. 또한 프로파일러 피드 서비스는 자동으로 비활성화됩니다.

오프라인 모드에서 피드 서비스를 수동으로 업데이트할 수도 있습니다. ISE 구축을 Cisco 피드 서비스에 연결할 수 없는 경우에는 이 옵션을 사용하여 업데이트를 수동으로 다운로드할 수 있습니다.

참고 라이선스가 60일 기간 내에 45일 동안 컴플라이언스를 벗어나면(OOC) 피드 서비스에서 업데이트를 수행할 수 없습니다. 라이선스가 만료되었거나 사용량이 허용되는 세션 수를 초과하면 라이선스가 컴플라이언스 상태가 아닙니다.

프로파일러 피드 서비스 구성

프로파일러 피드 서비스는 Cisco 피드 서버에서 신규 및 업데이트된 엔드포인트 프로파일링 정책과 MAC OUI 데이터베이스 업데이트를 검색합니다. 피드 서비스를 사용할 수 없거나 기타 오류가 발생한 경우에는 운영 감사 보고서에 해당 내용이 보고됩니다.

피드 서비스 사용 보고서를 Cisco로 다시 보내도록 Cisco ISE를 구성할 수 있습니다. 그러면 다음 정보가 Cisco로 전송됩니다.

- Hostname: Cisco ISE 호스트 이름
- MaxCount: 총 엔드포인트 수
- ProfiledCount: 프로파일이 지정된 엔드포인트 수
- UnknownCount: 알 수 없는 엔드포인트 수
- MatchSystemProfilesCount: Cisco에서 제공한 프로파일 수
- UserCreatedProfiles: 사용자가 생성한 프로파일 수

Cisco에서 제공한 프로파일링 정책에서 CoA 유형을 변경할 수 있습니다. 피드 서비스가 해당 정책을 업데이트할 때 CoA 유형은 변경되지 않지만 해당 정책의 나머지 속성은 업데이트됩니다.

Cisco ISE 릴리스 2.7 이상에서는 정책 업데이트를 다운로드하지 않고 OUI 업데이트를 수동으로 다운로드할 수 있습니다. 일부 프로파일러 조건을 CoA 유형 이상으로 변경하도록 맞춤 설정한 경우 프로파일러 피드가 이러한 조건을 대체하지 않도록 할 수 있습니다. OUI 업데이트를 계속 원할 수 있으므로 제조업체가 디바이스를 추가할 때 프로파일러가 새 디바이스를 식별할 수 있습니다. OUI만 다운로드하는 옵션은 피드 서비스 포털에서 사용할 수 있습니다.

시작하기 전에

프로파일러 피드 서비스는 분산형 구축이나 독립형 ISE 모드에서만 Cisco ISE 관리 포털에서 구성할 수 있습니다.

관리 포털(**Administration(**관리**)** > **System(**시스템**)** > **Settings(**설정**)**)에서 피드 업데이트에 대한 이메일 알림을 보내려는 경우 SMTP(Simple Mail Transfer Protocol) 서버를 설정합니다.

온라인에서 피드 서비스를 업데이트하려면 다음을 수행합니다.

단계 **1** **Administration(**관리**)** > **System(**시스템**)** > **Certificates(**인증서**)** > **Trusted Certificate(**신뢰할 수 있는 인증서**)** > **Import(**가져오기**)**를 선택합니다.

단계 **2** Work Centers Profiler Feeds (작업 센터 프로파일 러 피드)를 선택합니다. > > Administration FeedService Profiler (관리 FeedService 프로파일 러) 페이지의 옵션에 액세스 할 수도 있습니다. > >

단계 **3** **Online Subscription Update(**온라인 구독 업데이트**)** 탭을 클릭합니다.

단계 **4** **Test Feed Service Connection(**피드 서비스 연결 테스트**)** 버튼을 클릭하여 Cisco 피드 서비스에 연결되어 있으며 인증서가 유효한지 확인합니다.

단계 **5** **Enable Online Subscription Update(**온라인 구독 업데이트 활성화**)** 확인란을 선택합니다.

단계 **6** 시간을 HH:MM 형식(Cisco ISE 서버의 현지 표준 시간대)으로 입력합니다. 기본적으로 Cisco ISE 피드 서비스는 매일 오전 1시에 실행되도록 예약됩니다.

단계 **7** **Notify administrator when download occurs(**다운로드 수행 시 관리자에게 알림**)** 확인란을 선택하고 **Administrator email address(**관리자 이메일 주소**)** 텍스트 상자에 이메일 주소를 입력합니다. 민감하지 않은 정보(향후 릴리스에서 보다 나은 서비스와 추가적인 기능을 제공하는 데 사용할 예정)를 Cisco ISE가 수집하도록 허용하려면 **Provide Cisco anonymous information to help improve profiling accuracy(**프로파일링 정확도 개선을 위한 익명 정보를 **Cisco**에 제공**)** 확인란을 선택합니다.

단계 **8** **Save(**저장**)**를 클릭합니다.

단계 **9** **Update Now(**지금 업데이트**)**를 클릭합니다.

Cisco 피드 서버에 연결하여 마지막 피드 서비스 업데이트 이후 생성된 신규 및 업데이트된 프로파일이 있는지 확인하도록 Cisco ISE에 명령합니다. 그러면 시스템의 모든 엔드포인트가 다시 프로파일링되므로 시스템의 로드가 증가할 수 있습니다. 엔드포인트 프로파일링 정책이 업데이트되면 현재 Cisco ISE에 연결되어 있는 일부 엔드포인트의 권한 부여 정책이 변경될 수 있습니다.

마지막 피드 서비스 이후 생성되었으며 다운로드가 완료된 후에 활성화된 신규 및 업데이트된 프로파일을 업데이트할 때는 **Update Now(**지금 업데이트**)** 버튼이 비활성화됩니다. 프로파일러 피드 서비스의 컨피그레이션 창에서 이 창으로 돌아와야 합니다.

관련 항목

오프라인에서 프로파일러 피드 서비스 구성, 258 페이지

오프라인에서 프로파일러 피드 서비스 구성

Cisco ISE가 Cisco 피드 서버에 직접 연결할 수 없을 때는 오프라인으로 피드 서비스를 업데이트할 수 있습니다. Cisco 피드 서버에서 오프라인 업데이트 패키지를 다운로드하고 오프라인 피드 업데이트

를 사용하여 Cisco ISE에 업로드 할 수 있습니다. 또한 피드 서버에 추가된 새 정책에 대한 이메일 알림을 설정할 수도 있습니다.

오프라인으로 프로파일러 피드 서비스를 구성하려면 다음 작업을 수행합니다.

1. 오프라인 업데이트 패키지 다운로드
2. 오프라인 피드 업데이트 적용

오프라인 업데이트 패키지 다운로드

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Profiler(**프로파일러**)** > **Feeds(**피드**)**를 선택합니다.
Administration(관리**)** > **FeedService(**피드 서비스**)** > **Profiler(**프로파일러**)** 페이지에서 옵션에 액세스할 수도 있습니다.

단계 **2** **Offline Manual Update(**오프라인 수동 업데이트**)** 탭을 클릭합니다.

단계 **3** **Download Updated Profile Policies(**업데이트된 프로파일 정책 다운로드**)** 링크를 클릭합니다. 피드 서비스 파트너 포털로 리디렉션 됩니다.
브라우저에서 https://ise.cisco.com/partner/로 이동하여 피드 서비스 파트너 포털에 직접 방문할 수도 있습니다.

단계 **4** 처음 사용하는 경우 약관에 동의하십시오.
피드 서비스 관리자가 요청을 승인할 수 있도록 이메일이 트리거됩니다. 승인 시 확인 이메일이 전송됩니다.

단계 **5** Cisco.com 자격 증명을 사용하여 파트너 포털에 로그인합니다.

단계 **6** **Offline Feed(**오프라인 피드**) > Download Package(**패키지 다운로드**)**를 선택합니다.

단계 **7** **Generate Package(**패키지 생성**)**를 클릭합니다.

단계 **8** 생성된 패키지에 포함된 모든 프로파일 및 OUI를 보려면 **Click to View the Offline Update Package contents(**오프라인 업데이트 패키지 콘텐츠를 보려면 클릭**)** 링크를 클릭합니다.

- 피드 프로파일러 1 및 피드 OUI의 정책은 Cisco ISE의 모든 버전에 다운로드됩니다.
- 피드 프로파일러 2의 정책은 Cisco ISE 릴리스 1.3 이상에만 다운로드됩니다.
- 피드 프로파일러 3의 정책은 Cisco ISE 릴리스 2.1 이상에만 다운로드됩니다.

단계 **9** **Download Package(**패키지 다운로드**)**를 클릭하고 파일을 로컬 시스템에 저장합니다.
저장된 파일을 Cisco ISE 서버에 업로드하여 다운로드한 패키지에 피드 업데이트를 적용할 수 있습니다.

오프라인 피드 업데이트 적용

시작하기 전에

피드 업데이트를 적용하기 전에 오프라인 업데이트 패키지를 다운로드해야 합니다.

단계 **1** **Work Centers(**작업 센터**)** > **Profiler(**프로파일러**)** > **Feeds(**피드**)**Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 .

Administration(관리) > **FeedService(피드 서비스)** > **Profiler(프로파일러)**창에서 옵션에 액세스할 수도 있습니다.

단계 **2** **Offline Manual Update(오프라인 수동 업데이트)** 탭을 클릭합니다.

단계 **3** **Browse(찾아보기)**를 클릭하고 다운로드한 프로파일러 피드 패키지를 선택합니다.

단계 **4** **Apply Update(업데이트 적용)** 탭을 클릭합니다.

프로파일 및 OUI 업데이트를 위한 이메일 알림 구성

프로파일 및 OUI 업데이트에 대한 알림을 수신하도록 이메일 주소를 구성할 수 있습니다.

단계 **1** **Download Offline Update Package(오프라인 업데이트 패키지 다운로드)** 섹션의 **1** ~ 오프라인 업데이트 패키지 다운로드를 수행하여 피드 서비스 파트너 포털로 이동합니다.

단계 **2** **Offline Feed(오프라인 피드)** > **Email Preferences(이메일 환경 설정)**를 선택합니다.

단계 **3** 공지사항을 받으려면 **Enable Notifications(공지사항 사용)** 확인란을 선택합니다.

단계 **4** **days(일 수)** 드롭 다운 목록에서 일 수를 선택하여 새 업데이트에 대한 알림을 받을 빈도를 설정합니다.

단계 **5** 이메일 주소/우편 주소를 입력하고 **Save(저장)**를 클릭합니다.

피드 업데이트 취소

이전 업데이트에서 업그레이드된 엔드포인트 프로파일링 정책을 되돌리고 이전 Profiler Feed Service 업데이트를 통해 새로 추가된 OUI와 엔드포인트 프로파일링 정책을 제거할 수 있습니다. .

엔드포인트 프로파일링 정책은 피드 서버에서 업데이트한 후 수정해도 시스템에서 변경되지 않습니다.

단계 **1** Cisco ISE GUI에서 메뉴 아이콘(☰)을 클릭하고 **Work Centers(작업 센터)** > **Profiler(프로파일러)** > **Feeds(피드)**를 선택합니다.

단계 **2** **Go to Update Report Page(보고서 업데이트 페이지로 이동)**를 클릭하여 컨피그레이션 변경 감사 보고서에서 수행한 컨피그레이션 변경사항을 확인합니다.

단계 **3** **Undo Latest(최신 항목 취소)**를 클릭합니다.

프로파일러 보고서

Cisco ISE는 네트워크를 관리하는 데 사용할 수 있는 문제 해결 도구와 다양한 엔드포인트 프로파일링 관련 보고서를 제공합니다. 기록 데이터와 현재 데이터 둘 다에 대해 보고서를 생성할 수 있습니다. 보고서의 특정 부분을 드릴다운하여 추가 세부정보를 확인할 수도 있습니다. 큰 보고서의 경우에는 보고서를 예약하여 다양한 형식으로 다운로드할 수도 있습니다.

Operations(운영**) > Reports(**보고서**) > Endpoints and Users(**엔드포인트 및 사용자**)**에서 엔드포인트에 대한 다음 보고서를 실행할 수 있습니다.

- Endpoint Session History(엔드포인트 세션 기록)
- Profiled Endpoint Summary(프로파일링된 엔드포인트 요약)
- Endpoint Profile Changes(엔드포인트 프로파일 변경)
- Top Authorizations by Endpoint(엔드포인트별 상위 권한 부여)
- Registered Endpoints(등록된 엔드포인트)

엔드포인트의 비정상적인 동작 탐지

Cisco ISE는 MAC 주소의 불법 사용으로부터 네트워크를 보호합니다. Cisco ISE는 MAC 주소 스푸핑과 관련된 엔드포인트를 탐지하고 의심스러운 엔드포인트의 권한을 제한할 수 있습니다.

다음은 비정상적 동작에 대한 프로파일러 컨피그레이션 페이지의 두 가지 옵션입니다.

- 비정상적인 동작 탐지 활성화
- 비정상적인 동작 적용 활성화

비정상적인 동작 탐지를 활성화하는 경우 Cisco ISE는 데이터를 검사하고 NAS-Port-Type, DHCP 클래스 식별자 및 엔드포인트 정책과 관련된 속성의 변경 사항과 관련하여 기존 데이터와의 모순을 확인합니다. 그러한 경우 **AnomalousBehavior**라는 속성이 true로 설정된 엔드포인트에 추가되어 Visibility Context(가시성 상황) 페이지에서 엔드포인트를 필터링하고 볼 수 있습니다. 각 MAC 주소에 대한 감사 로그도 생성됩니다.

비정상적 동작 탐지가 활성화되면 Cisco ISE는 기존 엔드포인트의 다음 속성이 변경되었는지 확인합니다.

1. Port-Type(포트 유형)-엔드포인트의 액세스 방법이 변경되었는지 확인합니다. 이는 유선 Dot1x를 통해 연결된 동일한 MAC 주소가 무선 Dot1x에 사용된 경우 그리고 그 반대의 경우에만 적용됩니다.
2. DHCP Class Identifier(DHCP 클래스 식별자)-엔드포인트의 클라이언트 또는 벤더 유형이 변경되었는지 확인합니다. 이는 DHCP 클래스 식별자 속성이 특정 값으로 채워져 다른 값으로 변경된 경우에만 적용됩니다. 엔드포인트가 고정 IP로 구성된 경우 Cisco ISE에서 DHCP 클래스 식별자 속성이 비어 있습니다. 나중에 다른 디바이스가 이 엔드포인트의 MAC 주소를 스푸핑하고 DHCP를 사용하는 경우 클래스 식별자가 빈 값에서 특정 문자열로 변경됩니다. 이렇게 하면 비정상적 동작 탐지가 트리거되지 않습니다.
3. 엔드포인트 정책-중요한 프로파일 변경 사항이 있는지 확인합니다. 이는 엔드포인트의 프로파일이 "Phone(폰)" 또는 "Printer(프린터)"에서 "Workstation(워크 스테이션)"으로 변경된 경우에만 적용됩니다.

Anomalous Behavior Enforcement(비정상 동작 적용)를 활성화하는 경우 프로파일러 컨피그레이션 창에 구성된 권한 부여 규칙에 따라 의심스러운 엔드포인트를 다시 인증하는 데 사용할 수 있는 비정상 동작을 탐지하면 CoA가 실행됩니다.

비정상적인 동작이 있는 엔드포인트에 대한 권한 부여 정책 규칙 설정

Authorization Policy(권한 부여 정책) 페이지에서 해당 규칙을 설정하여 비정상적인 동작이 있는 엔드포인트에 대해 수행할 조치를 선택할 수 있습니다.

단계 **1** **Policy(**정책**) Policy Sets(**정책 집합**)**를 선택합니다.

단계 **2** 기본 정책에 해당하는 **View(**보기**)** 열에서 화살표 아이콘 을 클릭하여 보기 설정 화면을 열고 기본 권한 부여 정책을 보고 관리합니다.

단계 **3** 행의 **Actions(**작업**)** 열에서 톱니바퀴 아이콘을 클릭한 다음 드롭 다운 목록에서 필요에 따라 삽입 또는 복제 옵션을 선택하여 새 권한 부여 규칙을 삽입합니다.
정책 집합 표에 새 행이 표시됩니다.

단계 **4** Rule Name(규칙 이름)을 입력합니다.

단계 **5** **Conditions(**조건**)** 열에서 (+) 기호를 클릭합니다.

단계 **6** **Conditions Studio** 페이지에 필수 조건을 생성합니다. **Editor(**편집기**)** 섹션에서 **Click To Add an Attribute(**속성 추가 클릭**)** 텍스트 상자를 클릭하고 필요한 사전 및 속성(예: Endpoints.AnomalousBehaviorEqualsTrue)을 선택합니다.

Click To Add An Attribute(클릭하여 속성 추가**)** 텍스트 상자에 라이브러리 조건을 끌어다 놓을 수 있습니다.

단계 **7** **Use(**사용**)**를 클릭하여 비정상적인 동작이 있는 엔드포인트에 대한 권한 부여 정책 규칙 설정합니다.

단계 **8** **Done(**완료**)**을 클릭합니다.

비정상적인 동작이 있는 엔드포인트 보기

다음 옵션 중 하나를 사용하여 비정상적인 동작이 있는 엔드포인트를 볼 수 있습니다.

- **Home(**홈**)** > **Summary(**요약**)** > **Metrics(**메트릭**)**에서 Anomalous Behavior(비정상적인 동작)를 클릭합니다. 이 작업을 수행하면 창의 하단 패널에 Anomalous Behavior(비정상적인 동작) 열이 포함 된 새 탭이 열립니다.
- **Context Visibility(**상황 가시성**)** > **Endpoints(**엔드포인트**)** > **Endpoint Classification(**엔드포인트 분류**)**을 선택합니다. 창의 하단 패널에서 Anomalous Behavior(비정상적인 동작) 열을 볼 수 있습니다.
- 다음 단계에 설명된 대로 Context Visibility(상황 가시성) 창의 Authentication(인증) 보기 또는 Compromised Endpoints(침해 엔드포인트) 보기에서 Anomalous Behavior(비정상적인 동작) 열을 새로 생성할 수 있습니다.

단계 **1** **Context Visibility(**상황 가시성**)** > **Endpoints(**엔드포인트**)** > **Authentication(**인증**)** 또는 **Context Visibility(**상황 가시성**)** > **Endpoints(**엔드포인트**)** > **Compromised Endpoints(**침해 엔드포인트**)**를 선택합니다.

단계 **2** 창의 하단 패널에서 설정 아이콘을 클릭하고 **Anomalous Behavior(**비정상적인 동작**)** 확인란을 선택합니다.

단계 **3** **Go(**이동**)**를 클릭합니다.
Authentication(인증) 보기 또는 Compromised Endpoints(침해 엔드포인트) 보기에서 Anomalous Behavior(비정상적인 동작) 열을 볼 수 있습니다.

클라이언트 머신의 에이전트 다운로드 문제

문제

사용자 인증 및 권한 부여 후 클라이언트 머신 브라우저에 "일치하는 정책 없음" 오류 메시지가 표시됩니다. 이 문제는 인증의 클라이언트 프로비저닝 단계 중에 사용자 세션에 적용됩니다.

가능한 원인

클라이언트 프로비저닝 정책에 필요한 설정이 없습니다.

포스처 에이전트 다운로드 문제

포스처 에이전트 설치 프로그램을 다운로드하기 위해 필요한 사항은 다음과 같습니다.

- 사용자는 에이전트를 처음 클라이언트 머신에 설치할 때 브라우저 세션에서 ActiveX 설치 프로그램을 허용해야 합니다. 클라이언트 프로비저닝 다운로드 페이지에서 이에 대한 메시지가 표시됩니다.
- 클라이언트 머신에서 인터넷에 액세스할 수 있어야 합니다.

해결 방법

- 클라이언트 프로비저닝 정책이 Cisco ISE에 있는지 확인해 주십시오. 있는 경우 정책 ID 그룹, 조건 및 정책에 정의된 에이전트 유형을 확인합니다. (또한 프로파일에 모두 기본값이 적용되어 있더라도 **Policy(**정책**)** > **Policy Elements(**정책 요소**)** > **Results(**결과**)** > **Client Provisioning(**클라이언트 프로비저닝**)** > **Resources(**리소스**)Add(**추가**)AnyConnect Posture Profile(AnyConnect** 포스처 프로파일**)**에 에어전트 프로파일이 구성되어 있는지 여부를 확인해주십시오.)
- 액세스 스위치의 포트를 바운스하여 클라이언트 머신을 다시 인증해 보십시오.

엔드포인트

이러한 창에서는 네트워크에 연결하는 엔드포인트를 구성하고 관리할 수 있습니다.

엔드포인트 설정

다음 표에서는 엔드포인트를 생성하고 엔드포인트용 정책을 할당하는 데 사용할 수 있는 **Endpoints(**엔드포인트**)** 창의 필드에 대해 설명합니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Network Access(**네트워크 액세스**)** > **Identities(ID)** > **Endpoints(**엔드포인트**)**입니다.

표 ***59:*** 엔드포인트 설정

필드 이름	사용 지침
MAC Address(MAC 주소**)**	정적으로 엔드포인트를 생성하기 위한 MAC 주소를 16진수 형식으로 입력합니다. MAC 주소는 Cisco ISE가 활성화된 네트워크에 연결되어 있는 인터페이스의 디바이스 식별자입니다.
Static Assignment(정적 할당**)**	정적 할당 상태가 정적으로 설정되어 있을 때 엔드포인트 창에서 엔드포인트를 정적으로 생성하려면 이 확인란을 선택합니다. 엔드포인트의 정적 할당 상태는 정적에서 동적으로 또는 동적에서 정적으로 전환할 수 있습니다.
Policy Assignment(정책 할당**)**	(**Static Assignment(**정적 할당**)**가 선택되어 있지 않으면 기본적으로 비활성화됨) **Policy Assignment(**정책 할당**)** 드롭다운 목록에서 일치하는 엔드포인트 정책을 선택합니다. 다음 중 하나를 수행할 수 있습니다. • 일치하는 엔드포인트 정책을 선택하지 않고 기본 엔드포인트 정책인 Unknown(알 수 없음)을 사용하는 경우 엔드포인트의 동적 프로파일링을 허용하는 엔드포인트에 대해 정적 할당 상태가 동적으로 설정됩니다. • Unknown(알 수 없음) 이외의 일치하는 엔드포인트 정책을 선택하는 경우에는 해당 엔드포인트에 대해 정적 할당 상태가 정적으로 설정되며 **Static Assignment(**정적 할당**)** 확인란이 자동으로 선택됩니다.

필드 이름	사용 지침
Static Group Assignment(정적 그룹 할당**)**	엔드포인트를 ID 그룹에 정적으로 할당하려면 이 확인란을 선택합니다. 이 확인란을 선택하면 이전에 다른 엔드포인트 ID 그룹에 동적으로 할당되었던 엔드포인트에 대해 다음 번에 엔드포인트 정책을 평가하는 동안 프로파일링 서비스가 엔드포인트 ID 그룹을 변경하지 않습니다. 이 확인란의 선택을 취소하면 정책 컨피그레이션에 따라 엔드포인트 ID 그룹이 ISE 프로파일러가 할당한 대로 동적으로 설정됩니다. Static Group Assignment(정적 그룹 할당) 옵션을 선택하지 않으면 다음 번에 엔드포인트 정책을 평가하는 동안 엔드포인트가 일치하는 ID 그룹에 자동으로 할당됩니다.

Identity Group Assignment(ID 그룹 할당**)**	엔드포인트를 할당할 엔드포인트 ID 그룹을 선택합니다.
	
	엔드포인트에 대한 엔드포인트 정책 평가 중에 **Create Matching Identity Group(**일치하는 **ID** 그룹 생성**)** 옵션을 사용하지 않으려는 경우 또는 엔드포인트를 정적으로 생성하는 경우 ID 그룹에 엔드포인트를 할당할 수 있습니다.
	
	Cisco ISE에는 시스템에서 생성된 다음과 같은 엔드포인트 ID 그룹이 포함되어 있습니다.
	• Blocked List
	• GuestEndpoints
	• Profiled
	  • Cisco IP-Phone
	  • Workstation
	• RegisteredDevices
	• Unknown

관련 항목

식별된 엔드포인트, 251 페이지
정책 및 ID 그룹을 정적으로 할당하여 엔드포인트 생성, 246 페이지

LDAP에서 엔드포인트 가져오기 설정

다음 표에서는 LDAP 서버에서 엔드포인트를 가져오는 데 사용할 수 있는 Import from LDAP(LDAP에서 가져오기) 창의 필드에 대해 설명합니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Work Centers(**작업 센터**)** > **Network Access(**네트워크 액세스**)** > **Identities(ID)** > **Endpoints(**엔드포인트**)**입니다.

표 ***60: LDAP***에서 엔드포인트 가져오기 설정

필드 이름	사용 지침
Connection Settings(연결 설정**)**	
Host(호스트**)**	LDAP 서버의 호스트 이름 또는 IP 주소를 입력합니다.
Port(포트**)**	LDAP 서버의 포트 번호를 입력합니다. LDAP 서버에서 가져오려는 경우 기본 포트인 389를 사용할 수 있으며, SSL을 통해 LDAP 서버에서 가져오려는 경우 기본 포트인 636을 사용할 수 있습니다. 참고 Cisco ISE는 구성된 모든 포트 번호를 지원합니다. 구성된 값은 LDAP 서버 연결 세부정보와 일치해야 합니다.
Enable Secure Connection(보안 연결 활성화**)**	SSL을 통해 LDAP 서버에서 가져오려면 **Enable Secure Connection(**보안 연결 활성화**)** 확인란을 선택합니다.
Root CA Certificate Name(루트 **CA** 인증서 이름**)**	신뢰할 수 있는 CA 인증서를 보려면 드롭다운 화살표를 클릭합니다. 루트 CA 인증서 이름은 LDAP 서버에 연결하는 데 필요한 신뢰할 수 있는 CA 인증서를 지칭합니다. Cisco ISE에서는 신뢰할 수 있는 CA 인증서를 추가(가져오기), 편집, 삭제 및 내보내기할 수 있습니다.
Anonymous Bind(익명 바인딩**)**	**Anonymous Bind(**익명 바인딩**)** 확인란을 활성화하거나 slapd.conf 구성 파일에서 LDAP 관리자 자격 증명을 입력해야 합니다.
Admin DN(관리자 **DN)**	slapd.conf 구성 파일에서 LDAP 관리자에 대해 구성된 DN(Distinguished Name)을 입력합니다. 관리자 DN 형식의 예제는 cn=Admin, dc=cisco.com, dc=com과 같습니다.

필드 이름	사용 지침
Password(비밀번호**)**	slapd.conf 구성 파일에서 LDAP 관리자에 대해 구성된 비밀번호를 입력합니다.
Base DN(기본 **DN)**	부모 엔트리의 고유 이름을 입력합니다. 기본 DN 형식의 예제는 dc=cisco.com, dc=com과 같습니다.
Query Settings(쿼리 설정**)**	
MAC Address objectClass(MAC 주소 **objectClass)**	MAC 주소를 가져오는 데 사용되는 쿼리 필터(예: ieee802Device)를 입력합니다.
MAC Address Attribute Name(MAC 주소 속성 이름**)**	가져오려는 반환된 속성 이름(예: macAddress)을 입력합니다.
Profile Attribute Name(프로파일 속성 이름**)**	LDAP 속성의 이름을 입력합니다. 이 속성은 LDAP 서버에 정의되어 있는 각 엔드포인트 엔트리에 대한 정책 이름을 포함합니다. **Profile Attribute Name(**프로파일 속성 이름**)** 필드를 구성할 때는 다음 사항을 고려합니다. • **Profile Attribute Name(**프로파일 속성 이름**)** 필드에서 이 LDAP 속성을 지정하지 않거나 이를 잘못 구성하는 경우에는 가져오기 작업 중에 엔드포인트가 "알 수 없음"으로 표시되며 이러한 엔드포인트는 일치하는 엔드포인트 프로파일링 정책으로 별도로 프로파일이 지정됩니다. • **Profile Attribute Name(**프로파일 속성 이름**)** 필드에서 이 LDAP 속성을 구성하면 속성 값을 검증하여 엔드포인트 정책이 Cisco ISE의 기존 정책과 일치하는지를 확인한 다음, 엔드포인트를 가져옵니다. 엔드포인트 정책이 기존 정책과 일치하지 않으면 해당 엔드포인트를 가져오지 않습니다.
Time Out(시간 초과**)**	시간을 초 단위로 입력합니다. 유효한 범위는 1초 ~ 60초입니다.

관련 항목

식별된 엔드포인트, 251 페이지
LDAP 서버에서 엔드포인트 가져오기, 250 페이지

엔드포인트 프로파일링 정책 설정

다음 표에서는 **Endpoint Policies(**엔드포인트 정책**)** 창의 필드에 대해 설명합니다. 이 창을 보려면 메뉴 아이콘(☰)을 클릭하고 **Policy(**정책**)** > **Profiling(**프로파일링**)** > **Profiling Policies(**프로파일링 정책**)**입니다.

표 ***61:*** 엔드포인트 프로파일링 정책 설정

필드 이름	사용 지침
Name(이름**)**	생성하려는 엔드포인트 프로파일링 정책의 이름을 입력합니다.
Description(설명**)**	생성하려는 엔드포인트 프로파일링 정책의 설명을 입력합니다.
Policy Enabled(정책 활성화**)**	엔드포인트를 프로파일링할 때 일치하는 프로파일링 정책을 연결하기 위해 **Policy Enabled(**정책 활성화**)** 확인란은 기본적으로 선택됩니다. 이 확인란의 선택을 취소하면 엔드포인트 프로파일링 시 엔드포인트 프로파일링 정책이 제외됩니다.
Minimum Certainty Factor(최소 확실성 요인**)**	프로파일링 정책과 연결할 최소값을 입력합니다. 기본값은 10입니다.
Exception Action(예외 작업**)**	프로파일링 정책에서 규칙을 정의할 때 조건과 연결할 예외 작업을 선택합니다. 기본값은 NONE(없음)입니다. **Policy(**정책**) > Policy Elements(**정책 요소**) > Results(**결과**) > Profiling(**프로파일링**) > Exception Actions(**예외 작업**)**에서 예외 작업을 정의합니다.
Network Scan (NMAP) Action(네트워크 스캔 **(NMAP)** 작업**)**	필요한 경우 프로파일링 정책에서 규칙을 정의할 때 조건과 연결할 네트워크 스캔 작업을 목록에서 선택합니다. 기본값은 NONE(없음)입니다. **Policy(**정책**) > Policy Elements(**정책 요소**) > Results(**결과**) > Profiling(**프로파일링**) > Network Scan (NMAP) Actions(**네트워크 스캔**(NMAP)** 작업**)**에서 예외 작업을 정의합니다.

필드 이름	사용 지침
Create an Identity Group for the policy(정책에 대한 **ID** 그룹 생성**)**	엔드포인트 ID 그룹을 생성하려면 다음 옵션 중 하나를 선택합니다. • **Yes, create matching Identity Group(**예**,** 일치하는 **ID** 그룹을 생성합니다**.)** • **No, use existing Identity Group hierarchy(**아니요**,** 기존 **ID** 그룹 계층을 사용합니다**.)**
Yes, create matching Identity Group(예**,** 일치하는 **ID** 그룹을 생성합니다**.)**	기존 프로파일링 정책을 사용하려면 이 옵션을 선택합니다. 이 옵션을 선택하면 해당 엔드포인트에 대해 일치하는 ID 그룹이 생성되며, 엔드포인트 프로파일이 기존 프로파일링 정책과 일치하면 ID 그룹은 Profiled 엔드포인트 ID 그룹의 자식이 됩니다. 예를 들어 네트워크에서 검색된 엔드포인트가 Xerox-Device 프로파일과 일치하면 엔드포인트 ID 그룹 페이지에서 Xerox-Device 엔드포인트 ID 그룹이 생성됩니다.

필드 이름	사용 지침
No, use existing Identity Group hierarchy(아니요, 기존 **ID** 그룹 계층을 사용합니다**.)**	프로파일링 정책 및 ID 그룹의 계층 구성을 사용하여 일치하는 부모 엔드포인트 ID 그룹에 엔드포인트를 할당하려면 이 확인란을 선택합니다. 이 옵션을 사용하는 경우 엔드포인트 프로파일링 정책 계층을 사용하여 일치하는 부모 엔드포인트 ID 그룹 중 하나와 부모 ID 그룹에 대해 연결된 엔드포인트 ID 그룹에 엔드포인트를 할당할 수 있습니다. 예를 들어 기존 프로파일과 일치하는 엔드포인트는 적절한 부모 엔드포인트 ID 그룹 아래에 그룹화됩니다. 여기서 Unknown(알 수 없음) 프로파일과 일치하는 엔드포인트는 Unknown(알 수 없음) 아래에 그룹화되고 기존 프로파일과 일치하는 엔드포인트는 프로파일이 지정된 엔드포인트 ID 그룹 아래에 그룹화됩니다. 예를 들면 다음과 같습니다. • Cisco-IP-Phone 프로파일과 일치하는 엔드포인트는 Cisco-IP-Phone 엔드포인트 ID 그룹 아래에 그룹화됩니다. • Workstation 프로파일과 일치하는 엔드포인트는 Workstation 엔드포인트 ID 그룹 아래에 그룹화됩니다. Cisco-IP-Phone 및 Workstation 엔드포인트 ID 그룹은 시스템의 Profiled 엔드포인트 ID 그룹에 연결됩니다.
Parent Policy(부모 정책**)**	새 엔드포인트 프로파일링 정책을 연결할 시스템에 정의된 부모 프로파일링 정책을 선택합니다. 자식에게 규칙과 조건을 상속할 부모 프로파일링 정책을 선택할 수 있습니다.

필드 이름	사용 지침
Associated CoA Type(연결된 **CoA** 유형**)**	엔드포인트 프로파일링 정책과 연결할 CoA 유형을 다음 중에서 하나 선택합니다. • CoA 없음 • 포트 바운스 • 재인증 • Administration(관리) > System(시스템) > Settings(설정) > Profiling(프로파일링)에 설정된 프로파일러 컨피그레이션에서 적용되는 전역 설정
Rules(규칙**)**	엔드포인트 프로파일링 정책에 정의된 하나 이상의 규칙에 따라 엔드포인트에 일치하는 프로파일링 정책이 결정됩니다. 그러면 해당 프로파일에 따라 엔드포인트를 그룹화할 수 있습니다. 규칙에서는 정책 요소 라이브러리의 프로파일링 조건을 하나 이상 사용하여 전체 분류를 위한 엔드포인트 속성 및 해당 값을 검증합니다.

필드 이름	사용 지침
Conditions(조건**)**	고정된 Conditions(조건) 오버레이를 확장하려면 더하기 [+] 기호를 클릭하고, 고정된 오버레이를 닫으려면 빼기 [-] 기호를 클릭하거나 오버레이 바깥쪽을 클릭합니다. **Select Existing Condition from Library(**라이브러리에서 기존 조건 선택**)** 또는 **Create New Condition (Advanced Option)(**새 조건 생성**(**고급 옵션**))**을 클릭합니다. **Select Existing Condition from Library(**라이브러리에서 기존 조건 선택**)**: 정책 요소 라이브러리에서 미리 정의된 Cisco 조건을 선택하여 식을 정의할 수 있습니다. **Create New Condition (Advanced Option)(**새 조건 생성**(**고급 옵션**))**: 여러 시스템 또는 사용자 맞춤화 사전에서 속성을 선택하여 식을 정의할 수 있습니다. 다음 중 하나를 프로파일링 조건과 연결할 수 있습니다. • 각 조건에 대한 확실성 요인의 정수 값 • 해당 조건에 대한 예외 작업 또는 네트워크 스캔 작업 프로파일링 조건과 연결할 다음의 미리 정의된 설정 중 하나를 선택합니다. • Certainty Factor Increases(확실성 요인 증가): 각 규칙에 대한 확실성 값을 입력합니다. 전체 분류와 관련하여 모든 일치 규칙에 대해 이 값을 추가할 수 있습니다. • Take Exception Action(예외 작업 수행): 이 엔드포인트 프로파일링 정책의 Exception Action(예외 작업) 필드에 구성되어 있는 예외 작업을 트리거합니다. • Take Network Scan Action(네트워크 스캔 작업 수행): 이 엔드포인트 프로파일링 정책의 Network Scan (NMAP) Action(네트워크 스캔 (NMAP) 작업) 필드에 구성되어 있는 네트워크 스캔 작업을 트리거합니다.

필드 이름	사용 지침
Select Existing Condition from Library(라이브러리에서 기존 조건 선택**)**	다음을 수행할 수 있습니다. • 정책 요소 라이브러리에서 사용 가능한 미리 정의된 Cisco 조건을 선택한 다음 AND 또는 OR 연산자를 사용하여 여러 조건을 추가할 수 있습니다. • Action(작업) 아이콘을 클릭하여 후속 단계에서 다음을 수행합니다. • **Add Attribute or Value(**속성 또는 값 추가**)**: 임시 속성 또는 값 쌍을 추가할 수 있습니다. • **Add Condition from Library(**라이브러리에서 조건 추가**)**: 미리 정의된 Cisco 조건을 추가할 수 있습니다. • **Duplicate(**복제**)**: 선택한 조건의 복사본을 생성합니다. • **Add Condition to Library(**라이브러리에 조건 추가**)**: 생성한 임시 속성/값 쌍을 정책 요소 라이브러리에 저장할 수 있습니다. • **Delete(**삭제**)**: 선택한 조건을 삭제합니다.

필드 이름	사용 지침
Create New Condition (Advance Option)(새 조건 생성**(**고급 옵션**))**	다음을 수행할 수 있습니다. • 식에 임시 속성/값 쌍을 추가한 다음 AND 또는 OR 연산자를 사용하여 여러 조건을 추가할 수 있습니다. • Action(작업) 아이콘을 클릭하여 후속 단계에서 다음을 수행합니다. • **Add Attribute or Value(**속성 또는 값 추가**)**: 임시 속성 또는 값 쌍을 추가할 수 있습니다. • **Add Condition from Library(**라이브러리에서 조건 추가**)**: 미리 정의된 Cisco 조건을 추가할 수 있습니다. • **Duplicate(**복제**)**: 선택한 조건의 복사본을 생성합니다. • **Add Condition to Library(**라이브러리에 조건 추가**)**: 생성한 임시 속성/값 쌍을 정책 요소 라이브러리에 저장할 수 있습니다. • **Delete(**삭제**)**: 선택한 조건을 삭제합니다. AND 또는 OR 연산자를 사용할 수 있습니다.

관련 항목

Cisco ISE 프로파일링 서비스, 186 페이지
엔드포인트 프로파일링 정책 생성, 237 페이지
UDID 속성을 사용하는 엔드포인트 상황 가시성, 274 페이지

UDID 속성을 사용하는 엔드포인트 상황 가시성

고유 식별자(UDID)는 특정 엔드포인트의 MAC 주소를 식별하는 엔드포인트 속성입니다. 각 엔드포인트는 여러 MAC 주소를 가질 수 있습니다. 예를 들어 유선 인터페이스용 MAC 주소 하나와 무선 인터페이스용 MAC 주소 하나를 가질 수 있습니다. AnyConnect 에이전트는 해당 엔드포인트에 대한 UDID를 생성하고 이를 엔드포인트 속성으로 저장합니다. 권한 부여 쿼리에서 UDID를 사용할 수 있습니다. 각 엔드포인트의 UDID는 일정하게 유지되며, AnyConnect 설치 또는 제거 시 변경되지 않습니다. UUID를 사용하는 경우 **Context Visibility(**상황 가시성**)** 창(**Context Visibility(**상황 가시성**) > Endpoints(**엔드포인트**) > Compliance(**규정 준수**)**에서 NIC가 여러 개인 엔드포인트에 대해 여러 항목이 아닌 하나의 항목이 표시됩니다. Mac 주소가 아닌 특정 엔드포인트에서 포스처 제어를 보장할 수 있습니다.

참고 UDID를 생성하려면 엔드포인트에 AnyConnect 4.7 이상이 있어야 합니다.

Windows 및 Macintosh 엔드포인트용 엔드포인트 스크립트 마법사

엔드포인트 스크립트 마법사를 사용하면, 연결된 엔드포인트에서 스크립트를 실행하여 조직의 요구 사항을 준수하는 관리 작업을 수행할 수 있습니다. 여기에는 더 이상 사용되지 않는 소프트웨어 제거, 프로세스 또는 애플리케이션의 시작 또는 종료, 특정 서비스의 활성화 또는 비활성화 작업이 포함됩니다.

엔드포인트 스크립트는 Windows 및 Macintosh 엔드포인트에서 엔드포인트 스크립트 마법사를 통해 실행할 수 있습니다.

시작하기 전에

- 슈퍼 관리자의 사용자 역할이 있어야 합니다.
- 관리자 권한으로 Macintosh 및 Windows 엔드포인트에 액세스할 수 있도록 Cisco ISE에 대한 로그인 자격증명을 구성합니다.

  Cisco ISE GUI에서 **Menu(**메뉴**)** 아이콘(☰)을 클릭하고 **Administration(**관리**)** > **System(**시스템**)** > **Settings(**설정**)** > **Protocols(**프로토콜**)** > **Endpoint Login Configuration(**엔드포인트 로그인 구성**)**을 선택하여 다음을 구성합니다.

  - Cisco ISE가 엔드포인트에 로그인할 수 있는 도메인 자격 증명.
  - Cisco ISE가 로컬 사용자로 엔드포인트에 로그인할 수 있는 Windows 및 Macintosh용 로컬 사용자 자격증명.

    도메인 사용자가 로컬 사용자보다 우선합니다. 두 가지를 모두 구성했으며 로컬 사용자 자격증명으로 스크립트를 실행해야 하는 경우 도메인 자격증명을 제거해야 합니다.

- Windows 엔드포인트에는 Windows PowerShell 버전 5.1 이상이 설치되어 있어야 합니다. PowerShell 원격이 반드시 활성화되어 있어야 합니다.
- Macintosh 엔드포인트에는 Bash가 설치되어 있어야 합니다.
- Windows 및 Macintosh 엔드포인트 모두 cURL 버전 7.34 이상이 설치되어 있어야 합니다.
- Windows 및 Macintosh 엔드포인트는 네트워크에 연결되어야 하며 Cisco ISE에서 활성 세션이 있어야 합니다.

단계 **1** Cisco ISE GUI에서 **Menu(**메뉴**)** 아이콘(☰)을 클릭하고 **Context Visibility Endpoints(**상황 가시성 엔드포인트**)** > **Endpoints(**엔드포인트**)**를 선택합니다.

단계 **2** 창의 오른쪽 상단에 있는 링크 아이콘을 클릭하고 드롭 다운 목록에서 **Run Endpoint Scripts(**엔드포인트 스크립트 실행**)**를 선택합니다.

로그인 자격 증명을 아직 구성하지 않은 경우 **Welcome(**시작**)** 탭에 **Endpoint Login Configuration(**엔드포인트 로그인 컨피그레이션**)** 창에 대한 링크가 포함되어 있습니다. 로그인 자격 증명이 구성된 경우에만 이 탭의 오른쪽 하단에서 **Start(**시작**)** 버튼을 클릭할 수 있습니다.

단계 **3** **Select Category(**카테고리 선택**)** 탭에서 운영체제 또는 사용 가능한 애플리케이션을 기반으로 엔드포인트를 선택할 수 있습니다. **By OS(OS** 별**)** 또는 **By Application(**애플리케이션 별**)** 라디오 버튼을 클릭하여 선택합니다. **Next(**다음**)**를 클릭하여 작업을 계속합니다.

단계 **4** **Select Endpoints(**엔드포인트 선택**)** 창에서 대시릿이 OS 유형 또는 애플리케이션에 사용 가능한 필터를 표시합니다. 대시릿에서 적용할 필터를 클릭하면 해당 필터의 모든 엔드포인트가 표에 나열됩니다.

- 선택한 필터에 대한 모든 엔드포인트를 선택하려면 표의 제목 행에 있는 확인란을 선택합니다.
- 특정 엔드포인트를 선택하려면 표에서 해당 항목의 확인란을 선택합니다. 표에서 특정 엔드포인트를 찾으려면 표 위의 **Filter(**필터**)** 버튼을 클릭하고 **Quick Filter(**빠른 필터**)**를 선택합니다. 표시된 엔드포인트를 기준으로 필터링하여 필요한 엔드포인트를 찾을 수 있습니다.

참고 **Select Categories(**카테고리 선택**)** 단계에서 **By Application(**애플리케이션 기준**)**을 선택한 경우 이 단계에서 동일한 OS 유형에 속하는 엔드포인트를 선택해야 합니다. 애플리케이션 기반 스크립트의 경우 각 OS 유형에 대한 스크립트를 생성하고 엔드포인트 스크립트 마법사에서 각 OS 유형에 대해 별도의 작업을 설정합니다.

단계 **5** 스크립트를 실행할 엔드포인트를 선택한 후 **Next(**다음**)**를 클릭합니다.

단계 **6** **Select Scripts(**스크립트 선택**)** 탭에서 **Add(**추가**)**를 클릭합니다.

단계 **7** **Add Script(**스크립트 추가**)**를 클릭하여 시스템에서 스크립트를 선택합니다. **Start Upload(**업로드 시작**)**를 클릭하여 **Select Scripts(**스크립트 선택**)** 탭에 스크립트를 추가합니다.

단계 **8** 실행할 스크립트의 확인란을 선택하고 **Next(**다음**)**를 클릭합니다.

단계 **9** **Summary(**요약**)** 탭에는 선택한 엔드포인트 및 선택한 스크립트가 표시됩니다. 여기에서 선택 항목을 검토하고 **Back(**뒤로**)**을 클릭하여 세부정보를 변경합니다. **Finish(**종료**)**를 클릭하여 스크립트 실행을 시작합니다.

이 작업의 작업 **ID**와 함께 **Endpoints Script Report(**엔드포인트 스크립트 보고서**)** 팝업 창이 표시됩니다. 이 작업의 세부정보가 포함된 창으로 리디렉션할 **Endpoint Scripts provisioning report(**엔드포인트 스크립트 프로비저닝 보고서**)**를 클릭합니다.

엔드포인트 스크립트 마법사를 통해 실행되는 작업의 보고서를 보려면 **Operations(**운영**)** > **Reports(**보고서**)** > **Reports(**보고서**)** > **Endpoints and Users(**엔드포인트 및 사용자**)** > **Endpoint Scripts Provisioning Summary(**엔드포인트 스크립트 프로비저닝 요약**)**을 선택합니다.

엔드포인트 스크립트 프로비저닝 요약 보고서

Cisco ISE GUI에서 **Menu(**메뉴**)** 아이콘(☰)을 클릭하고 **Operations(**작업**)** > **Reports(**보고서**)** > **Reports(**보고서**)** > **Endpoints and Users(**엔드포인트 및 사용자**)** > **Endpoint Scripts Provisioning Summary(**엔드포인트 스크립트 프로비저닝 요약**)**를 선택합니다.

엔드포인트 스크립트 프로비저닝 요약 창에는 지난 30일간 엔드포인트 스크립트 마법사를 통해 실행된 작업의 세부정보가 표시됩니다. 창 내보내기를 예약하고 이전 보고서를 추적하려면 창의 오른쪽 상단에서 **Schedule(**일정**)**을 클릭합니다.

Export To(내보내기 대상**)**를 클릭하고 드롭다운 목록에서 보고서의 CSV 또는 PDF 버전을 저장소 또는 로컬 대상에 저장하는 옵션을 선택합니다.

Endpoint Scripts Provisioning Summary(엔드 포인트 스크립트 프로비저닝 요약**)** 창에는 기본적으로 다음 열이 포함된 표가 표시됩니다.

이름 열	표시되는 정보
로그인 시간	작업 제출 타임 스탬프.
작업 **ID**	이 항목의 세부정보를 보려면 Job ID(작업 ID) 항목을 클릭합니다. 엔드포인트 스크립트 프로비저닝 세부정보가 포함된 새 탭이 열리고 타임 스탬프, 선택한 엔드포인트의 MAC 주소, 각 엔드포인트에 대한 스크립트 상태 및 프로비저닝 상태, 작업을 프로비저닝하는 PSN의 이름 및 작업 ID가 함께 표시됩니다. 참고 참고: 스크립트 실행에 대한 상세한 단계별 세부정보를 보려면 MAC 주소를 클릭합니다.
관리자 이름	작업을 제출한 관리자의 이름.
Operating System(운영체제**)**	선택한 스크립트가 실행되는 운영체제.
총/성공/실패/진행 중인 엔드포인트	• 선택한 총 엔드포인트 수. • 스크립트가 성공적으로 실행된 엔드포인트의 수. • 스크립트 실행에 실패한 엔드포인트의 수. • 스크립트가 아직 실행중인 엔드포인트의 수.
스크립트 이름	작업에 포함된 스크립트의 이름.

IF-MIB

객체	**OID**
ifIndex	1.3.6.1.2.1.2.2.1.1
ifDescr	1.3.6.1.2.1.2.2.1.2
ifType	1.3.6.1.2.1.2.2.1.3
ifSpeed	1.3.6.1.2.1.2.2.1.5

객체	OID
ifPhysAddress	1.3.6.1.2.1.2.2.1.6
ifAdminStatus	1.3.6.1.2.1.2.2.1.7
ifOperStatus	1.3.6.1.2.1.2.2.1.8

SNMPv2-MIB

객체	OID
system	1.3.6.1.2.1.1
sysDescr	1.3.6.1.2.1.1.1.0
sysObjectID	1.3.6.1.2.1.1.2.0
sysUpTime	1.3.6.1.2.1.1.3.0
sysContact	1.3.6.1.2.1.1.4.0
sysName	1.3.6.1.2.1.1.5.0
sysLocation	1.3.6.1.2.1.1.6.0
sysServices	1.3.6.1.2.1.1.7.0
sysORLastChange	1.3.6.1.2.1.1.8.0
sysORTable	1.3.6.1.2.1.1.9.0

IP-MIB

객체	OID
ipAdEntIfIndex	1.3.6.1.2.1.4.20.1.2
ipAdEntNetMask	1.3.6.1.2.1.4.20.1.3
ipNetToMediaPhysAddress	1.3.6.1.2.1.4.22.1.2
ipNetToPhysicalPhysAddress	1.3.6.1.2.1.4.35.1.4

CISCO-CDP-MIB

객체	OID
cdpCacheEntry	1.3.6.1.4.1.9.9.23.1.2.1.1
cdpCacheIfIndex	1.3.6.1.4.1.9.9.23.1.2.1.1.1
cdpCacheDeviceIndex	1.3.6.1.4.1.9.9.23.1.2.1.1.2
cdpCacheAddressType	1.3.6.1.4.1.9.9.23.1.2.1.1.3
cdpCacheAddress	1.3.6.1.4.1.9.9.23.1.2.1.1.4
cdpCacheVersion	1.3.6.1.4.1.9.9.23.1.2.1.1.5
cdpCacheDeviceId	1.3.6.1.4.1.9.9.23.1.2.1.1.6
cdpCacheDevicePort	1.3.6.1.4.1.9.9.23.1.2.1.1.7
cdpCachePlatform	1.3.6.1.4.1.9.9.23.1.2.1.1.8
cdpCacheCapabilities	1.3.6.1.4.1.9.9.23.1.2.1.1.9
cdpCacheVTPMgmtDomain	1.3.6.1.4.1.9.9.23.1.2.1.1.10
cdpCacheNativeVLAN	1.3.6.1.4.1.9.9.23.1.2.1.1.11
cdpCacheDuplex	1.3.6.1.4.1.9.9.23.1.2.1.1.12
cdpCacheApplianceID	1.3.6.1.4.1.9.9.23.1.2.1.1.13
cdpCacheVlanID	1.3.6.1.4.1.9.9.23.1.2.1.1.14
cdpCachePowerConsumption	1.3.6.1.4.1.9.9.23.1.2.1.1.15
cdpCacheMTU	1.3.6.1.4.1.9.9.23.1.2.1.1.16
cdpCacheSysName	1.3.6.1.4.1.9.9.23.1.2.1.1.17
cdpCacheSysObjectID	1.3.6.1.4.1.9.9.23.1.2.1.1.18
cdpCachePrimaryMgmtAddrType	1.3.6.1.4.1.9.9.23.1.2.1.1.19
cdpCachePrimaryMgmtAddr	1.3.6.1.4.1.9.9.23.1.2.1.1.20
cdpCacheSecondaryMgmtAddrType	1.3.6.1.4.1.9.9.23.1.2.1.1.21
cdpCacheSecondaryMgmtAddr	1.3.6.1.4.1.9.9.23.1.2.1.1.22
cdpCachePhysLocation	1.3.6.1.4.1.9.9.23.1.2.1.1.23
cdpCacheLastChange	1.3.6.1.4.1.9.9.23.1.2.1.1.24

CISCO-VTP-MIB

객체	OID
vtpVlanIfIndex	1.3.6.1.4.1.9.9.46.1.3.1.1.18.1
vtpVlanName	1.3.6.1.4.1.9.9.46.1.3.1.1.4.1
vtpVlanState	1.3.6.1.4.1.9.9.46.1.3.1.1.2.1

CISCO-STACK-MIB

객체	OID
portIfIndex	1.3.6.1.4.1.9.5.1.4.1.1.11
vlanPortVlan	1.3.6.1.4.1.9.5.1.9.3.1.3.1

BRIDGE-MIB

객체	OID
dot1dTpFdbPort	1.3.6.1.2.1.17.4.3.1.2
dot1dBasePortIfIndex	1.3.6.1.2.1.17.1.4.1.2

OLD-CISCO-INTERFACE-MIB

객체	OID
locIfReason	1.3.6.1.4.1.9.2.2.1.1.20

CISCO-LWAPP-AP-MIB

객체	OID
cLApEntry	1.3.6.1.4.1.9.9.513.1.1.1
cLApSysMacAddress	1.3.6.1.4.1.9.9.513.1.1.1.1.1
cLApIfMacAddress	1.3.6.1.4.1.9.9.513.1.1.1.1.2

객체	OID
cLApMaxNumberOfDot11Slots	1.3.6.1.4.1.9.9.513.1.1.1.1.3
cLApEntPhysicalIndex	1.3.6.1.4.1.9.9.513.1.1.1.1.4
cLApName	1.3.6.1.4.1.9.9.513.1.1.1.1.5
cLApUpTime	1.3.6.1.4.1.9.9.513.1.1.1.1.6
cLLwappUpTime	1.3.6.1.4.1.9.9.513.1.1.1.1.7
cLLwappJoinTakenTime	1.3.6.1.4.1.9.9.513.1.1.1.1.8
cLApMaxNumberOfEthernetSlots	1.3.6.1.4.1.9.9.513.1.1.1.1.9
cLApPrimaryControllerAddressType	1.3.6.1.4.1.9.9.513.1.1.1.1.10
cLApPrimaryControllerAddress	1.3.6.1.4.1.9.9.513.1.1.1.1.11
cLApSecondaryControllerAddressType	1.3.6.1.4.1.9.9.513.1.1.1.1.12
cLApSecondaryControllerAddress	1.3.6.1.4.1.9.9.513.1.1.1.1.13
cLApTertiaryControllerAddressType	1.3.6.1.4.1.9.9.513.1.1.1.1.14
cLApTertiaryControllerAddress	1.3.6.1.4.1.9.9.513.1.1.1.1.15
cLApLastRebootReason	1.3.6.1.4.1.9.9.513.1.1.1.1.16
cLApEncryptionEnable	1.3.6.1.4.1.9.9.513.1.1.1.1.17
cLApFailoverPriority	1.3.6.1.4.1.9.9.513.1.1.1.1.18
cLApPowerStatus	1.3.6.1.4.1.9.9.513.1.1.1.1.19
cLApTelnetEnable	1.3.6.1.4.1.9.9.513.1.1.1.1.20
cLApSshEnable	1.3.6.1.4.1.9.9.513.1.1.1.1.21
cLApPreStdStateEnabled	1.3.6.1.4.1.9.9.513.1.1.1.1.22
cLApPwrInjectorStateEnabled	1.3.6.1.4.1.9.9.513.1.1.1.1.23
cLApPwrInjectorSelection	1.3.6.1.4.1.9.9.513.1.1.1.1.24
cLApPwrInjectorSwMacAddr	1.3.6.1.4.1.9.9.513.1.1.1.1.25
cLApWipsEnable	1.3.6.1.4.1.9.9.513.1.1.1.1.26
cLApMonitorModeOptimization	1.3.6.1.4.1.9.9.513.1.1.1.1.27
cLApDomainName	1.3.6.1.4.1.9.9.513.1.1.1.1.28
cLApNameServerAddressType	1.3.6.1.4.1.9.9.513.1.1.1.1.29
cLApNameServerAddress	1.3.6.1.4.1.9.9.513.1.1.1.1.30

객체	OID
cLApAMSDUEnable	1.3.6.1.4.1.9.9.513.1.1.1.1.31
cLApEncryptionSupported	1.3.6.1.4.1.9.9.513.1.1.1.1.32
cLApRogueDetectionEnabled	1.3.6.1.4.1.9.9.513.1.1.1.1.33

CISCO-LWAPP-DOT11-CLIENT-MIB

객체	OID
cldcClientEntry	1.3.6.1.4.1.9.9.599.1.3.1.1
cldcClientMacAddress	1.3.6.1.4.1.9.9.599.1.3.1.1.1
cldcClientStatus	1.3.6.1.4.1.9.9.599.1.3.1.1.2
cldcClientWlanProfileName	1.3.6.1.4.1.9.9.599.1.3.1.1.3
cldcClientWgbStatus	1.3.6.1.4.1.9.9.599.1.3.1.1.4
cldcClientWgbMacAddress	1.3.6.1.4.1.9.9.599.1.3.1.1.5
cldcClientProtocol	1.3.6.1.4.1.9.9.599.1.3.1.1.6
cldcAssociationMode	1.3.6.1.4.1.9.9.599.1.3.1.1.7
cldcApMacAddress	1.3.6.1.4.1.9.9.599.1.3.1.1.8
cldcIfType	1.3.6.1.4.1.9.9.599.1.3.1.1.9
cldcClientIPAddress	1.3.6.1.4.1.9.9.599.1.3.1.1.10
cldcClientNacState	1.3.6.1.4.1.9.9.599.1.3.1.1.11
cldcClientQuarantineVLAN	1.3.6.1.4.1.9.9.599.1.3.1.1.12
cldcClientAccessVLAN	1.3.6.1.4.1.9.9.599.1.3.1.1.13
cldcClientLoginTime	1.3.6.1.4.1.9.9.599.1.3.1.1.14
cldcClientUpTime	1.3.6.1.4.1.9.9.599.1.3.1.1.15
cldcClientPowerSaveMode	1.3.6.1.4.1.9.9.599.1.3.1.1.16
cldcClientCurrentTxRateSet	1.3.6.1.4.1.9.9.599.1.3.1.1.17
cldcClientDataRateSet	1.3.6.1.4.1.9.9.599.1.3.1.1.18

CISCO-AUTH-FRAMEWORK-MIB

객체	OID
cafPortConfigEntry	1.3.6.1.4.1.9.9.656.1.2.1.1
cafSessionClientMacAddress	1.3.6.1.4.1.9.9.656.1.4.1.1.2
cafSessionStatus	1.3.6.1.4.1.9.9.656.1.4.1.1.5
cafSessionDomain	1.3.6.1.4.1.9.9.656.1.4.1.1.6
cafSessionAuthUserName	1.3.6.1.4.1.9.9.656.1.4.1.1.10
cafSessionAuthorizedBy	1.3.6.1.4.1.9.9.656.1.4.1.1.12
cafSessionAuthVlan	1.3.6.1.4.1.9.9.656.1.4.1.1.14

EEE8021-PAE-MIB: RFC IEEE 802.1X

객체	OID
dot1xAuthAuthControlledPortStatus	1.0.8802.1.1.1.1.2.1.1.5
dot1xAuthAuthControlledPortControl	1.0.8802.1.1.1.1.2.1.1.6
dot1xAuthSessionUserName	1.0.8802.1.1.1.1.2.4.1.9

HOST-RESOURCES-MIB

객체	OID
hrDeviceDescr	1.3.6.1.2.1.25.3.2.1.3
hrDeviceStatus	1.3.6.1.2.1.25.3.2.1.5

LLDP-MIB

객체	OID
lldpEntry	1.0.8802.1.1.2.1.4.1.1
lldpTimeMark	1.0.8802.1.1.2.1.4.1.1.1
lldpLocalPortNum	1.0.8802.1.1.2.1.4.1.1.2

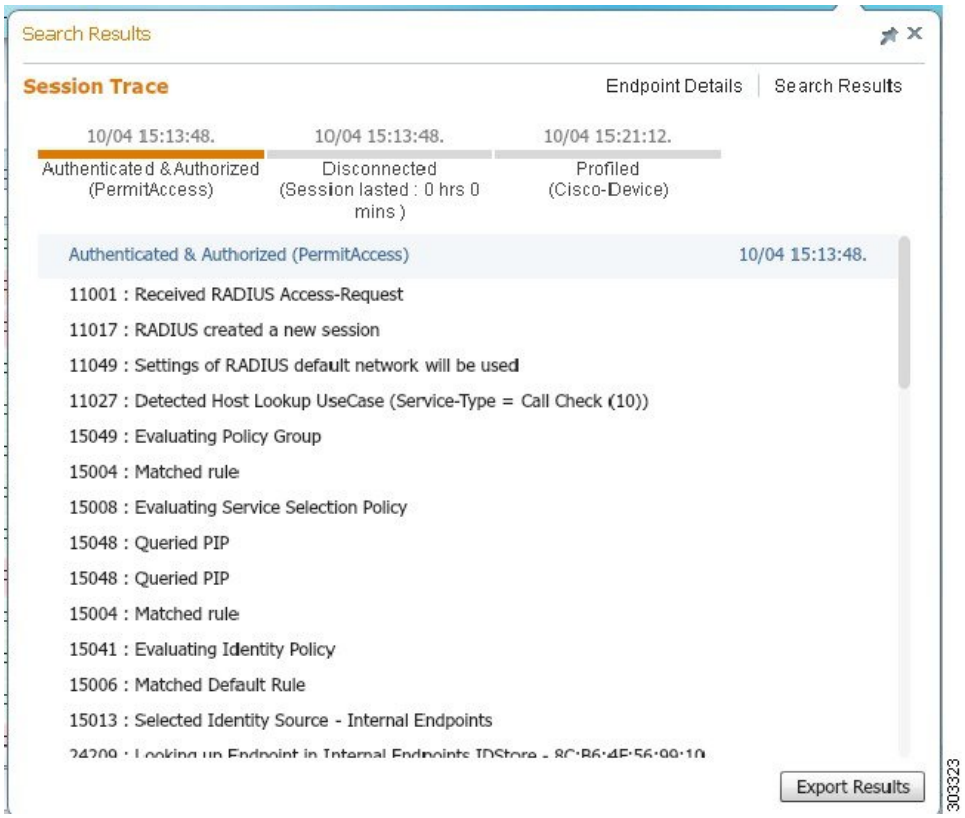
객체	**OID**
lldpIndex	1.0.8802.1.1.2.1.4.1.1.3
lldpChassisIdSubtype	1.0.8802.1.1.2.1.4.1.1.4
lldpChassisId	1.0.8802.1.1.2.1.4.1.1.5
lldpPortIdSubtype	1.0.8802.1.1.2.1.4.1.1.6
lldpPortId	1.0.8802.1.1.2.1.4.1.1.7
lldpPortDescription	1.0.8802.1.1.2.1.4.1.1.8
lldpSystemName	1.0.8802.1.1.2.1.4.1.1.9
lldpSystemDescription	1.0.8802.1.1.2.1.4.1.1.10
ldpCapabilitiesMapSupported	1.0.8802.1.1.2.1.4.1.1.11
lldpCacheCapabilities	1.0.8802.1.1.2.1.4.1.1.12

엔드포인트에 대한 세션 추적

Cisco ISE 홈 페이지 위쪽에 있는 글로벌 검색 상자를 사용하여 특정 엔드포인트의 세션 정보를 가져올 수 있습니다. 특정 기준으로 검색하는 경우 엔드포인트 목록이 표시됩니다. 이러한 엔드포인트 중 하나를 클릭하여 해당 엔드포인트에 대한 세션 추적 정보를 볼 수 있습니다. 다음 그림에는 엔드포인트에 대해 표시되는 세션 추적 정보의 예가 나와 있습니다.

참고 검색에 사용되는 데이터 집합은 엔드포인트 ID를 색인으로 사용합니다. 그러므로 인증이 발생할 때 인증에서 검색 결과 집합에 그러한 ID를 포함하도록 엔드포인트의 엔드포인트 ID가 반드시 있어야 합니다.

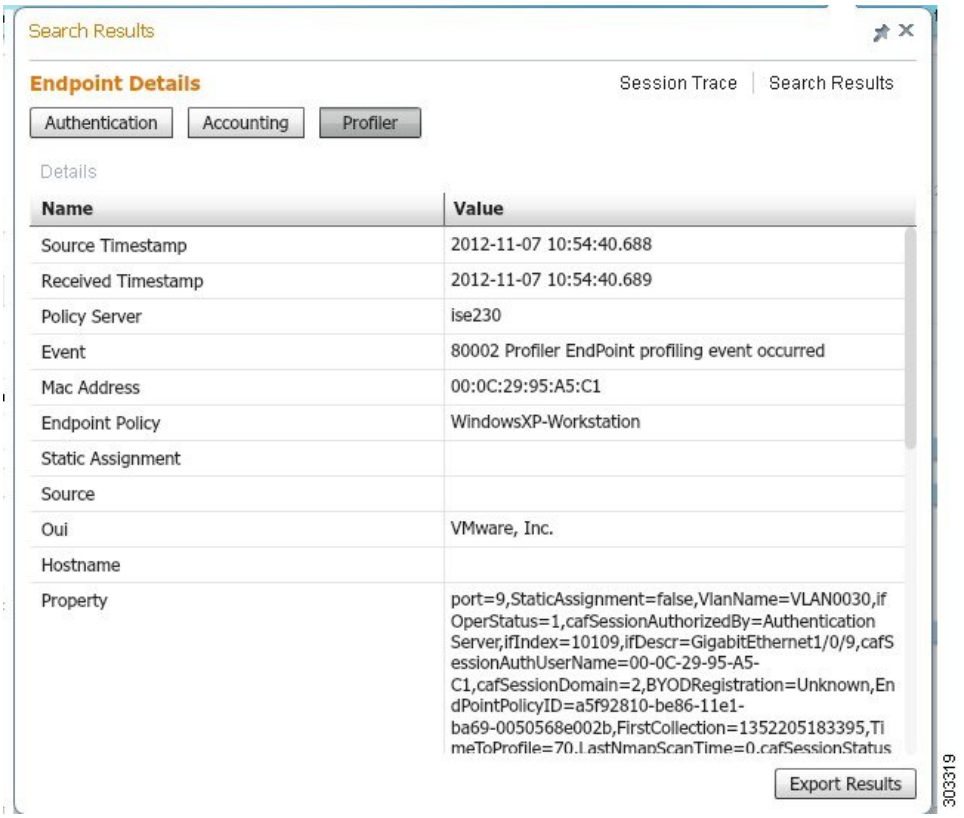
그림 ***16:*** 엔드포인트의 세션 추적



상단에 있는 클릭 가능한 타임라인을 사용하여 주요 권한 부여 전환을 볼 수 있습니다. **Export Results(**결과 내보내기**)** 옵션을 사용하여 .csv 형식으로 결과를 내보낼 수도 있습니다. 보고서는 브라우저로 다운로드됩니다.

Endpoint Details(엔드포인트 세부정보**)** 링크를 클릭하여 특정 엔드포인트에 대한 자세한 인증, 계정 관리 및 프로파일러 정보를 볼 수 있습니다. 다음 그림에는 엔드포인트에 대해 표시되는 엔드포인트 세부정보의 예가 나와 있습니다.

그림 *17:* 엔드포인트 세부정보



디렉토리에서 세션 제거

세션은 모니터링 및 문제 해결 노드의 세션 디렉토리에서 다음과 같이 지워집니다.

- 종료된 세션은 종료된 지 15분 후에 지워집니다.
- 인증은 있지만 계정 관리가 없는 세션은 1시간 후에 지워집니다.
- 모든 비활성 세션은 5일 이후에 지워집니다.

엔드포인트에 대한 글로벌 검색

Cisco ISE 홈 페이지 위쪽에 있는 글로벌 검색 상자를 사용하여 엔드포인트를 검색할 수 있습니다. 다음 조건을 사용하여 엔드포인트를 검색할 수 있습니다.

- 사용자 이름
- MAC 주소
- IP 주소

- 권한 부여 프로파일
- 엔드포인트 프로파일
- 실패 이유
- ID 그룹
- ID 저장소
- 네트워크 디바이스 이름
- 네트워크 디바이스 유형
- 운영체제
- 포스처 상태
- 위치
- 보안 그룹
- 사용자 유형

데이터를 표시하려면 Search(검색) 필드에 검색 기준으로 3자 이상을 입력해야 합니다.

참고 Cisco ISE에서 엔드포인트를 인증했거나 계정 관리 업데이트를 수신한 경우 전역 검색을 통해 엔드포인트를 찾을 수 있습니다. 수동으로 추가되었고 Cisco ISE에서 인증되지 않았거나 계정이 처리되지 않은 엔드포인트는 검색 결과에 표시되지 않습니다.

검색 결과에서는 엔드포인트의 현재 상태를 한 눈에 볼 수 있는 자세한 정보를 제공하므로 이 정보를 사용하여 문제를 해결할 수 있습니다. 검색 결과로는 상위 25개 항목만 표시됩니다. 필터를 사용하여 결과 범위를 좁히는 것이 좋습니다.

좌측 패널의 속성을 사용하여 결과를 필터링할 수 있습니다. 또한 원하는 엔드포인트를 클릭하여 다음과 같이 엔드포인트에 대한 자세한 정보를 확인할 수 있습니다.

- 세션 추적
- 인증 세부정보
- 계정 관리 세부정보
- 포스처 세부정보
- 프로파일러 세부정보
- 클라이언트 프로비저닝 세부정보
- 게스트 계정 관리 및 활동