Management Center의

management center에는 웹 및 CLI 액세스에 필요한 기본 관리자 계정이 포함되어 있습니다. 이 장에서는 맞춤형 사용자 계정을 생성하는 방법을 설명합니다.

사용자 정보

매니지드 디바이스에서 맞춤형 사용자 계정을 내부 사용자로 추가할 수 있으며, LDAP 또는 RADIUS 서버에 외부 사용자로 추가할 수 있습니다. 매니지드 디바이스 각각은 별도 사용자 계정을 유지 관리합니다. 예를 들어 사용자를 management center에 추가하는 경우, 해당 사용자만 management center에 액세스할 수 있습니다. 해당 사용자 이름을 사용해 매니지드 디바이스에 직접 로그인할 수 없습니다. 매니지드 디바이스에서 사용자를 별도로 추가해야 합니다.

내부 및 외부 사용자

매니지드 디바이스는 두 가지 유형의 사용자를 지원합니다.

- 내부 사용자—디바이스는 사용자 인증을 위해 로컬 데이터베이스를 검사합니다.
- 외부 사용자—사용자가 로컬 데이터베이스에 없는 경우, 시스템이 외부 LDAP 또는 RADIUS 인증 서버에 쿼리합니다.

사용자 역할

CLI 사용자 역할

management center의 CLI 외부 사용자는 사용자 역할이 없습니다. CLI 사용자는 사용 가능한 명령을 모두 사용할 수 있습니다.

웹 인터페이스 사용자 역할

CDO(Cisco Defense Orchestrator)에는 읽기 전용, 편집 전용, 구축 전용, 관리자, 슈퍼 관리자 등 다양한 사용자 역할이 있습니다. 사용자 역할은 각 테넌트의 각 사용자에 대해 구성됩니다. CDO 사용자가 둘 이상의 테넌트에 액세스할 수 있는 경우, 사용자 ID는 동일하지만 테넌트마다 역할이 다를 수 있습니다. 사용자는 한 테넌트에 대해서는 읽기 전용 역할을, 다른 테넌트에서는 슈퍼 관리자 역할을 가질 수 있습니다. 인터페이스 또는 설명서에서 읽기 전용 사용자, Deploy Only(구축 전용), Edit Only(수정 전용), Admin 사용자 또는 Super Admin 사용자를 언급하는 경우 특정 테넌트에 대한 사용자의 권한 수준을 의미합니다.

Read Only(읽기 전용**)**

읽기 전용 사용자는 정책 및 개체를 수정할 수 없으며 디바이스에 변경 사항을 구축할 수 없으며 보기만 가능합니다.

Deploy Only(구축 전용**)**

Deploy Only(구축 전용) 사용자는 디바이스 또는 여러 디바이스에 단계적 변경 사항을 구축하는 모든 정책 및 개체를 볼 수 있습니다.

Edit Only(편집 전용**)**

Edit Only(편집 전용) 사용자는 정책 및 개체를 수정하고 저장할 수 있지만 디바이스에 구축할 수는 없습니다.

Super Admin and Admin(슈퍼 관리자 및 관리자**)**

Super Admin and Admin(슈퍼 관리자 및 관리자) 사용자는 제품의 모든 항목에 액세스할 수 있습니다. 이 사용자는 모든 정책 및 개체를 생성, 읽기, 수정 및 삭제할 수 있으며 디바이스에 구축할 수 있습니다.

CDO 사용자 이름으로 CDO 사용자 레코드 생성

"슈퍼 관리자" 권한이 있는 CDO 사용자만 CDO 사용자 레코드를 생성할 수 있습니다. 슈퍼 관리자는 위의 **Create Your CDO Username(CDO** 사용자 이름 생성**)** 작업에서 지정한 것과 동일한 이메일 주소로 사용자 레코드를 만들어야 합니다.

적절한 사용자 역할이 있는 사용자 레코드를 생성하려면 다음 절차를 수행합니다.

Procedure

단계 **1** CDO에 로그인합니다.

단계 **2** CDO 메뉴 모음에서 **Settings(**설정**)** > **User Management(**사용자 관리**)**를 선택합니다.

단계 **3** 파란색 더하기  버튼을 클릭하여 새 사용자를 테넌트에 추가합니다.

단계 **4** 사용자의 이메일 주소를 입력합니다.

Note 사용자의 이메일 주소는 Cisco Secure Log-On 계정의 이메일 주소와 일치해야 합니다.

단계 **5** 드롭다운 메뉴에서 사용자 역할을 선택합니다.

단계 **6** **OK(**확인**)**를 클릭합니다.

Management Center에 대한 외부 인증 구성

외부 인증을 활성화하려면 하나 이상의 외부 인증 개체를 추가해야 합니다.

Management Center에 대한 외부 인증 정보

외부 인증을 활성화하는 경우, 외부 인증 개체에 지정된 대로 management center에서 LDAP 또는 RADIUS 서버로 사용자 자격 증명을 확인합니다.

웹 인터페이스 액세스를 위한 여러 외부 인증 개체를 구성할 수 있습니다. 예를 들어 외부 인증 개체가 5개인 경우, 그러한 개체에서 사용자는 웹 인터페이스 액세스를 인증받을 수 있습니다. CLI 액세스는 외부 인증 개체를 하나만 사용할 수 있습니다. 외부 인증 개체를 하나 이상 활성화하는 경우, 사용자는 목록에서 첫 번째 개체로만 인증할 수 있습니다.

management center의 경우, 외부 인증 객체를 **System(**시스템**)** > **User(**사용자**)** > **External Authentication(**외부 인증**)** 탭에서 직접 활성화합니다. 이 설정은 management center 사용에만 영향을 주며 매니지드 디바이스 사용에 대해 이 탭에서 활성화할 필요는 없습니다. threat defense 디바이스의 경우, 디바이스에 구축하는 플랫폼 설정에서 외부 인증 객체를 활성화해야 합니다.

웹 인터페이스 사용자는 내부 인증 개체에 있는 CLI 사용자와 별개로 정의됩니다. RADIUS의 CLI 사용자의 경우, 외부 인증 개체의 RADIUS 사용자 이름목록을 사전 구성해야 합니다. LDAP의 경우, 필터를 지정하여 LDAP 서버의 CLI 사용자와 매칭할 수 있습니다.

참고 CLI 액세스 권한이 있는 사용자는 **expert** 명령을 사용하여 Linux 셸에 액세스할 수 있습니다. Linux 셸 사용자는 루트 권한을 얻을 수 있으며, 따라서 보안 위험이 발생할 수 있습니다. 다음을 확인하십시오.

- CLI 또는 Linux 셸 액세스 권한이 있는 사용자 목록 제한
- Linux 셸 사용자를 생성하지 마십시오.

LDAP 정보

LDAP(Lightweight Directory Access Protocol)를 사용하면 중앙의 한 위치에 개체(예: 사용자 크리덴셜)를 조직하는 네트워크에서 디렉토리를 설정할 수 있습니다. 그러면 여러 애플리케이션에서 이 크리덴셜 및 크리덴셜 설명에 사용된 정보에 액세스할 수 있습니다. 사용자 크리덴셜을 변경해야 하는 경우, 한 곳에서 변경할 수 있습니다.

Microsoft는 Active Directory 서버가 2020년에 LDAP 바인딩 및 LDAP 서명을 시행할 것이라고 발표했습니다. Microsoft는 이러한 설정을 기본 설정으로 사용할 때 Microsoft Windows에 권한 상승 취약점

이 존재하여 MITM(man-in-the-middle) 공격자가 Windows LDAP 서버에 인증 요청을 성공적으로 전달할 수 있기 때문에 이러한 요구 사항을 적용하고 있습니다. 자세한 내용은 Microsoft 지원 사이트에서 2020 LDAP 채널 바인딩 및 Windows용 LDAP 서명 요구 사항을 참조하십시오.

아직 수행하지 않은 경우 TLS/SSL 암호화를 사용하여 Active Directory 서버에서 인증을 시작하는 것이 좋습니다.

RADIUS 정보

RADIUS(Remote Authentication Dial In User Service)는 네트워크 리소스에 대한 사용자 액세스의 인증, 권한 부여, 어카운팅에 사용되는 인증 프로토콜입니다. RFC 2865를 준수하는 모든 RADIUS 서버에 대해 인증 개체를 생성할 수 있습니다.

Firepower 디바이스는 SecurID 토큰 사용을 지원합니다. SecurID를 사용하여 서버에서 인증을 구성하는 경우, 해당 서버에서 인증된 사용자는 SecurID PIN 끝에 SecurID 토큰을 추가하고 이를 로그인 비밀번호로 사용합니다. SecurID를 지원하기 위해 Firepower 디바이스에서 추가로 구성할 사항은 없습니다.

CDO에 대한 LDAP 외부 인증 개체 추가

LDAP 서버를 추가하고 디바이스 관리를 위해 외부 사용자를 지원합니다.

다중 도메인 구축에서 외부 인증 개체는 생성된 도메인에서만 사용할 수 있습니다.

시작하기 전에

- 해당 장치에서 도메인 이름 조회를 위해 DNS 서버를 지정해야 합니다. 이 절차에서 IP 주소는 지정하고 LDAP 서버에 대한 호스트 이름은 지정하지 않더라도, LDAP 서버는 인증을 위한 URI를 반환할 수 있으며 여기에는 호스트 이름이 포함됩니다. 호스트 이름을 지정하려면 DNS 조회가 필요합니다.
- CAC 인증과 함께 사용할 LDAP 인증 개체를 구성하는 경우 컴퓨터에 삽입된 AC를 제거해서는 안 됩니다. 사용자 인증서를 활성화한 다음에는 항상 CAC가 삽입된 상태여야 합니다.

프로시저

단계 **1** 시스템 (⚙) > **Users**(사용자)을 선택합니다.
단계 **2** **External Authentication**(외부 인증) 탭을 클릭합니다.
단계 **3** **Add External Authentication Object**(외부 인증 개체 추가)를 클릭합니다.
단계 **4** **Authentication Method**(인증 방법)을 **LDAP**로 설정합니다.
단계 **5** **Name**(이름)과 **Description**(설명)(선택 사항)을 입력합니다.
단계 **6** 드롭다운 목록에서 **Server Type**(서버 유형)을 선택합니다.

팁 **Set Defaults(**기본 설정**)**을 클릭하면 디바이스가 **User Name Template(**사용자 이름 템플릿**)**, **UI Access Attribute(UI** 액세스 속성**)**, **CLI Access Attribute(CLI** 액세스 속성**)**, **Group Member Attribute(**그룹 구성원 속성**)** 및 **Group Member URL Attribute(**그룹 구성원 **URL** 속성**)** 필드를 서버 유형의 기본값으로 채웁니다.

단계 **7** **Primary Server(**기본 서버**)**에 **Host Name/IP Address(**호스트 이름**/IP** 주소**)**를 입력합니다.

TLS 또는 SSL을 통한 연결에 인증서를 사용하는 경우 인증서의 호스트 이름이 이 필드에 사용된 호스트 이름과 일치해야 합니다. 또한 IPv6 주소는 암호화된 연결이 지원되지 않습니다.

단계 **8** (선택 사항) **Port(**포트**)**를 기본값에서 변경합니다.

단계 **9** (선택 사항) **Backup Server(**백업 서버**)** 파라미터를 입력합니다.

단계 **10** **LDAP-Specific Parameters(LDAP** 전용 파라미터**)**를 입력합니다.

a) 액세스를 원하는 LDAP 디렉터리에 대해 **Base DNs(**기본 **DN)**를 입력합니다. 예를 들어, 예시 회사의 보안 조직에서 이름을 인증하려면 `ou=security,dc=example,dc=com`을 입력합니다. 아니면 **Fetch DN(DN** 가져오기**)**을 클릭하고, 드롭다운 목록에서 적절한 기본 고유 이름을 선택합니다.

b) (선택 사항) **Base Filter(**기본 필터**)**를 입력합니다. 예를 들어 디렉토리 트리의 사용자 개체에 `physicalDeliveryOfficeName` 속성이 있고 뉴욕 사무실의 사용자는 그 속성 값이 `NewYork`인 경우 뉴욕 사무실의 사용자만 가져오려면 `(physicalDeliveryOfficeName=NewYork)`이라고 입력합니다.

CAC 인증을 사용하는 경우 활성 사용자 계정만 필터링하려면(비활성화된 사용자 계정 제외) `(!(userAccountControl:1.2.840.113556.1.4.803:=2))`를 입력합니다. 이 기준은 `ldpgrp` 그룹에 속하는 AD 내에서 사용자 계정을 검색하며 `userAccountControl` 속성 값이 `2`(비활성화됨)가 아닙니다.

c) LDAP 서버를 검색하기에 크리덴셜이 충분한 사용자의 경우, **User Name(**사용자 이름**)**을 입력합니다. 예를 들어 OpenLDAP 서버에 연결하려는 경우, 해당 사용자 개체에 `uid` 속성이 있으며 예시 회사 보안 부서 관리자 개체의 `uid`값이 `NetworkAdmin`이라면 `uid=NetworkAdmin,ou=security,dc=example,dc=com`과 같이 입력할 수 있습니다.

d) **Password(**비밀번호**)** 및 **Confirm Password(**비밀번호 확인**)** 필드에 사용자 비밀번호를 입력합니다.

e) (선택 사항) **Show Advanced Options(**고급 옵션 표시**)**를 클릭하고 다음 고급 옵션을 구성합니다.

- **Encryption(**암호화**)- None (**해당 없음**)**, **TLS**또는 **SSL**을 클릭 합니다.

  포트를 지정한 다음 암호화 방식을 변경할 경우, 그 방법에 대해서는 포트가 기본값으로 재설정됩니다. **None(**해당 없음**)** 또는 **TLS**인 경우, 포트는 기본값인 389로 재설정됩니다. SSL 암호화를 선택할 경우 포트는 636로 재설정됩니다.

- **SSL Certificate Upload Path(SSL** 인증서 업로드 경로**)**—SSL 또는 TLS 암호화인 경우, **Choose File(**파일 선택**)**을 클릭하여 인증서를 선택해야 합니다.

  이전에 업로드한 인증서를 대체하려는 경우, 새 인증서를 업로드하고 구성을 디바이스에 다시 적용하여 새 인증서로 복사합니다.

  참고 TLS 암호화는 모든 플랫폼에서 인증서가 필요합니다. 항상 끼어들기 공격을 방지하기 위해 SSL에 대한 인증서를 업로드하는 것이 좋습니다.

- **User Name Template(**사용자 이름 템플릿**)**— **UI Access Attribute(UI** 액세스 속성**)**에 해당하는 템플릿을 제공합니다. 예를 들어 예시 회사의 보안 조직에서 근무하는 모든 사용자를 인증하기 위해 UI 액세스 속성이 `uid`인 OpenLDP 서버에 연결하는 경우, `uid=%s,ou=security,dc=example,dc=com`를 **User Name Template(**사용자 이름 템플릿**)** 필드에 입력합니다. Microsoft Active Directory 서버에서는 `%s@security.example.com`이라고 입력할 수 있습니다.

  이 필드는 CAC 인증을 위해 필요합니다.

- **Shell User Name Template(**쉘 사용자 이름 템플릿**)**— CLI 사용자 인증을 위해 **CLI Access Attribute(CLI** 액세스 속성**)**에 해당하는 템플릿을 제공합니다. 예를 들어 보안 조직에서 근무하는 모든 사용자를 인증하기 위해 CLI 액세스 속성이 `sAMAccountName`인 OpenLDP 서버에 연결하는 경우, `%s`를 **Shell User Name Template(**쉘 사용자 이름 템플릿**)** 필드에 입력합니다.

- **Timeout(**시간 초과**)**—백업 연결로 전환하기 전 시간(초)을 1과 1024 사이로 입력합니다. 기본값은 30입니다.

  참고 시간 초과 범위는 threat defense와 management center에 따라 다르므로 개체를 공유하는 경우 threat defense의 더 작은 시간 초과 범위 (1 ~ 30초)를 초과하지 않아야 합니다. 시간 초과 값을 더 높은 값으로 설정하면 threat defense LDAP 구성이 작동하지 않습니다.

단계 **11** (선택 사항) **Attribute Mapping(**속성 매핑**)**을 구성하고 속성에 따라 사용자를 검색합니다.

- **UI Access Attribute(UI** 액세스 속성**)**을 입력하거나 **Fetch Attrs(**속성 가져오기**)**를 클릭하여 사용 가능한 속성 목록을 검색합니다. 예를 들어 Microsoft Active Directory Server의 경우 Active Directory Server 사용자 개체에 `uid` 속성이 없기 때문에 UI Access Attribute(UI 액세스 속성)를 사용하여 사용자를 검색할 수도 있습니다. 그 대신 `userPrincipalName` 속성을 검색할 수 있는데, `userPrincipalName`을 **UI Access Attribute(UI** 액세스 속성**)** 필드에 입력하면 됩니다.

- 사용자 고유 유형 이외의 쉘(shell) 액세스 속성을 사용하려는 경우 **CLI Access Attribute(CLI** 액세스 속성**)**를 입력합니다. 예를 들어 `sAMAccountName` CLI 액세스 속성을 사용하여 셸 액세스 사용자를 가져오려면 `sAMAccountName`을 입력합니다.

단계 **12** (선택 사항) **Group Controlled Access Roles(**그룹 제어 액세스 역할**)**를 구성합니다.

액세스 제어 그룹에 역할을 사용하여 사용자의 권한을 구성하지 않는 경우, 사용자는 외부 인증 정책에서 기본적으로 부여된 권한만 갖습니다.

a) (선택 사항) 사용자 역할에 해당하는 필드에 해당 역할이 부여되는 사용자를 포함하는 LDAP 그룹의 DN을 입력합니다.

   참조하는 모든 그룹이 LDAP 서버에 있어야 합니다. 고정 LDAP 그룹 또는 동적 LDAP 그룹을 참조할 수 있습니다. 고정 LDAP 그룹은 특정 사용자를 가리키는 그룹 개체 특성에 의해 멤버십이 결정되며, 동적 LDAP 그룹에서는 사용자 개체 특성에 따라 그룹 사용자를 가져오는 LDAP 검색을 생성하여 멤버십을 결정합니다. 어떤 역할에 대한 그룹 액세스 권한은 그룹의 멤버인 사용자에게만 영향을 미칩니다.

동적 그룹을 사용하는 경우 LDAP 서버에 구성된 대로 LDAP 쿼리가 사용됩니다. 이런 이유로 Firepower 디바이스는 검색 반복 횟수를 4회로 제한하여 검색 구문 오류로 인한 무한 루프를 방지합니다.

예제**:**

Administrator(관리자**)** 필드에 다음과 같이 입력하여 예시 회사의 정보 기술 조직에서 이름을 인증할 수 있습니다.

```
cn=itgroup,ou=groups, dc=example,dc=com
```

b) 지정된 어떤 그룹에도 속하지 않는 사용자에 대해 **Default User Role(**기본 사용자 역할**)**을 선택합니다.

c) 정적 그룹을 사용하는 경우, **Group Member Attribute(**그룹 멤버 속성**)**을 입력합니다.

예제**:**

기본 Security Analyst 액세스에 대한 고정 그룹의 멤버십을 표시하기 위해 `member(멤버)` 속성을 사용하는 경우 `member(멤버)`라고 입력합니다.

d) 동적 그룹을 사용하는 경우, **Group Member URL Attribute(**그룹 멤버 **URL** 속성**)**을 입력합니다.

예제**:**

`memberURL` 속성이 기본 관리자 액세스에 대해 지정한 동적 그룹의 멤버를 가져오는 LDAP 검색을 포함할 경우 `memberURL`이라고 입력합니다.

단계 **13** (선택 사항) CLI 사용자를 허용하도록 **CLI Access Filter(CLI** 액세스 필터**)**를 설정합니다.

CLI 액세스에 대해 LDAP 인증을 하지 않으려면 이 필드를 비워 둡니다. CLI 사용자를 지정하려면 다음 방법 중 하나를 선택합니다.

- 인증 설정을 구성할 때 지정한 것과 동일한 필터를 사용하려면 **Same as Base Filter(**기본 필터와 동일**)**를 선택합니다.
- 속성 값에 따라 관리자 사용자 엔트리를 검색하려면 속성 이름, 비교 연산자, 필터로 사용할 속성 값을 괄호로 묶어 입력합니다. 예를 들어 모든 네트워크 관리자에게 `manager` 속성이 있고 그 값이 `shell`이라면 `(manager=shell)`이라는 기본 필터를 설정할 수 있습니다.

사용자 이름은 다음과 같은 Linux 기준을 준수해야 합니다.

- 최대 32개의 영숫자 문자와 하이픈(-) 및 밑줄(_)
- 모두 소문자
- 하이픈(-)으로 시작할 수 없으며, 숫자만으로 구성할 수 없고, 마침표(.), 단가 기호(@) 또는 슬래시(/)를 포함할 수 없음

참고 CLI 액세스 권한이 있는 사용자는 **expert** 명령을 사용하여 Linux 셸에 액세스할 수 있습니다. Linux 셸 사용자는 루트 권한을 얻을 수 있으며, 따라서 보안 위험이 발생할 수 있습니다. CLI 또는 Linux 셸 액세스 권한을 갖는 사용자의 목록을 제한해야 합니다.

참고 **CLI Access Filter(CLI** 액세스 필터**)**에 포함된 사용자와 사용자 이름이 동일한 내부 사용자를 만들지 마십시오. 내부 management center 사용자만 관리자여야 합니다. **CLI Access Filter(CLI** 액세스 필터**)**에 관리자를 포함하지 마십시오.

단계 **14** (선택 사항) **Test(**테스트**)**를 클릭하고 LDAP 서버와의 연결을 테스트합니다.

테스트 출력에서는 유효한 사용자 이름과 유효하지 않은 사용자 이름을 나열합니다. 사용자 이름은 고유해야 하며 밑줄(_), 마침표(.), 하이픈(-), 영숫자를 포함할 수 있습니다. 1,000명이 넘는 사용자로 서버와의 연결을 테스트할 경우 UI 페이지 크기 제한 때문에 1,000명의 사용자만 반환됩니다. 테스트에 실패하는 경우 LDAP 인증 연결 문제 해결, 17 페이지을 참조하십시오.

단계 **15** (선택 사항) **Additional Test Parameters(**추가 테스트 파라미터**)**를 입력하고 인증 가능한 사용자의 크리덴셜을 테스트할 수도 있습니다. **User Name(**사용자 이름**)** `uid` 및 **Password(**비밀번호**)**를 입력한 다음 **Test(**테스트**)**를 클릭합니다.

Microsoft Active Directory Server에 연결하는 경우 `uid` 대신 UI 액세스 속성을 제공했다면 해당 속성의 값을 사용자 이름으로 사용합니다. 해당 사용자의 정규화된 DN을 지정할 수도 있습니다.

팁 테스트 사용자의 이름이나 비밀번호를 잘못 입력할 경우 서버 구성이 맞더라도 테스트는 실패합니다. 서버 구성이 올바른지 확인하려면 먼저 **Test(**테스트**)**를 클릭합니다. 여기서 **Additional Test Parameters(**추가 테스트 파라미터**)** 필드에는 사용자 정보를 입력할 필요가 없습니다. 테스트가 성공하면 사용자 이름과 비밀번호를 입력하고 특정 사용자로 테스트하십시오.

예제**:**

예를 들어 예시 회사의 `JSmith` 사용자 크리덴셜을 가져올 수 있는지 테스트하려면 `JSmith`를 입력하고 올바른 비밀번호를 입력합니다.

단계 **16** **Save(**저장**)**를 클릭합니다.

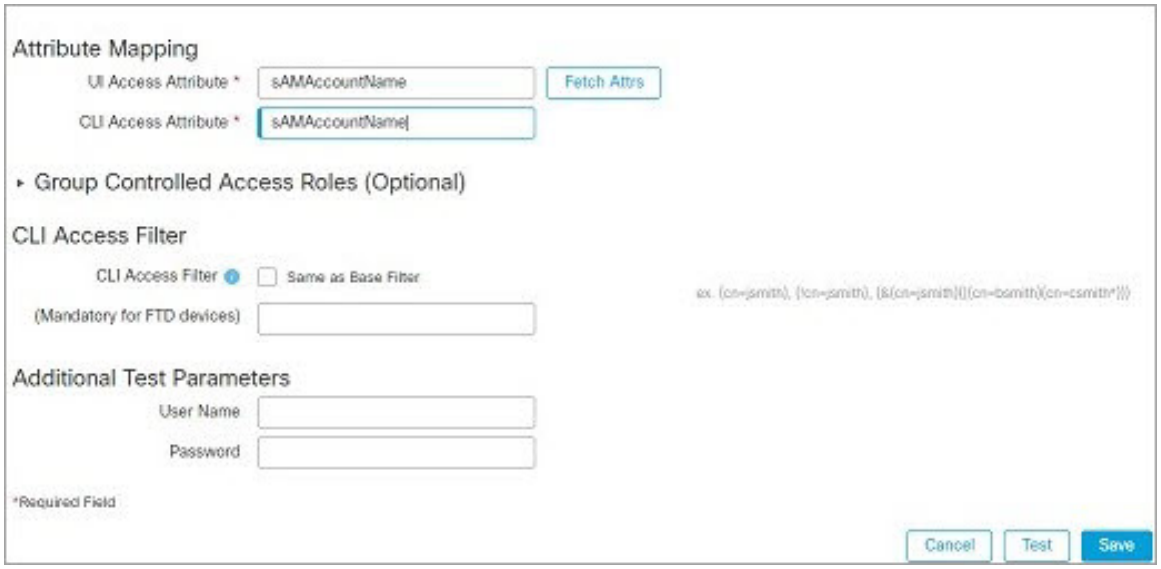
단계 **17** 이 서버의 사용을 활성화합니다. CDO 사용자에 대한 외부 인증 활성화, 16 페이지를 참조하십시오.

예

기본 예시

다음 그림은 Microsoft Active Directory Server를 위한 LDAP 로그인 인증 개체의 기본 구성입니다. 여기서 LDAP 서버의 IP 주소는 10.11.3.4입니다. 이 연결은 포트 389을 액세스에 사용합니다.

이 예는 예시 회사의 정보 기술 도메인에 있는 보안 조직에 대해 `OU=security,DC=it,DC=example,DC=com`이라는 기본 DN을 사용하는 연결을 보여줍니다.



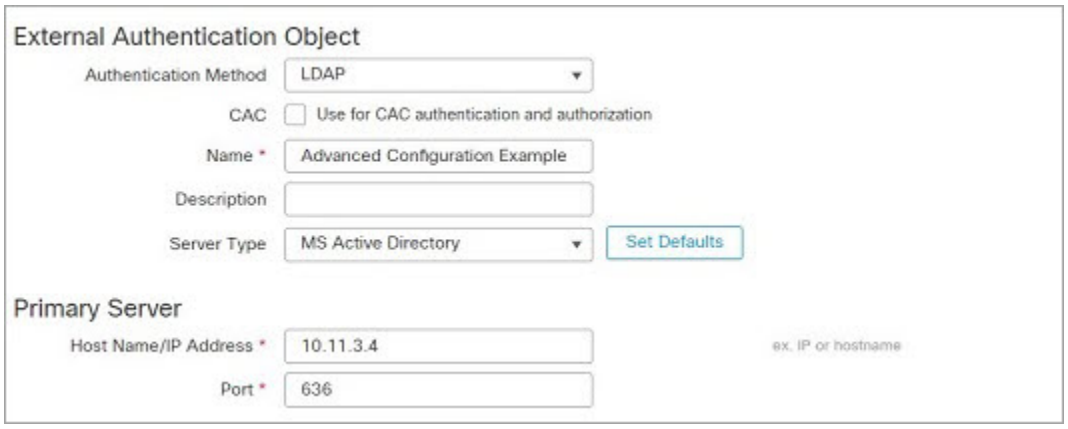
그러나 이 서버는 Microsoft Active Directory Server이므로 `sAMAccountName` 속성을 사용해 사용자 이름을 저장하며 `uid` 속성을 사용하지 않습니다. MS Active Directory Server 유형을 선택하고 **Set Defaults(**기본값 설정**)**을 클릭하면 UI Access Attribute(UI 액세스 속성)이 `sAMAccountName`으로 설정됩니다. 이에 따라 시스템에서는 사용자가 시스템에 대한 로그인을 시도하는 경우 각 개체에 대해 `sAMAccountName` 속성을 검사하면서 사용자 이름을 매칭합니다.

또한 CLI액세스 속성이 `sAMAccountName`이면 사용자가 어플라이언스의 CLI 계정에 로그인할 때 디렉터리의 모든 개체에 대해 각 `sAMAccountName`속성을 검사하여 매칭하는지 확인합니다.

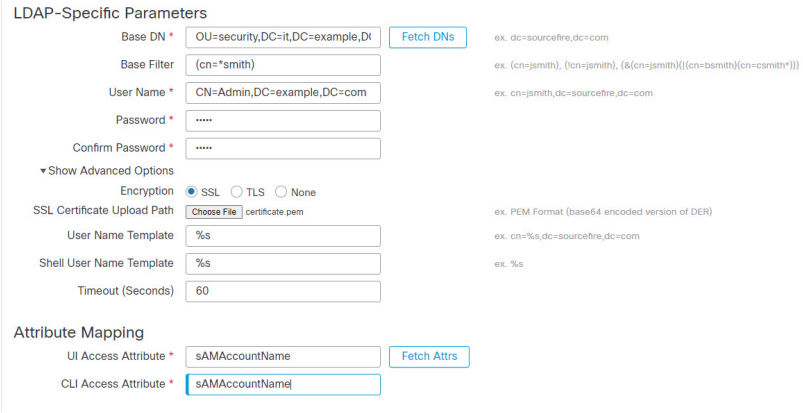
이 서버에는 기본 필터가 적용되지 않으므로 시스템은 기본 DN이 나타내는 디렉터리의 모든 개체에 대해 속성을 검사합니다. 기본 기간(또는 LDAP 서버에 설정된 시간 초과 기간)이 경과하면 서버와의 연결이 시간 초과됩니다.

고급 예시

이 예에서는 Microsoft Active Directory Server에 대한 LDAP 로그인 인증 개체의 고급 구성을 보여줍니다. 여기서 LDAP 서버의 IP 주소는 10.11.3.4입니다. 이 연결은 포트 636을 액세스에 사용합니다.



이 예는 예시 회사의 정보 기술 도메인에 있는 보안 조직에 대해 `OU=security,DC=it,DC=example,DC=com`이라는 기본 DN을 사용하는 연결을 보여줍니다. 그러나 이 서버는 기본 필터 `(cn=*smith)`가 있습니다. 이 필터는 CN이 `smith`로 끝나는 사용자만 서버에서 가져오도록 제한합니다.

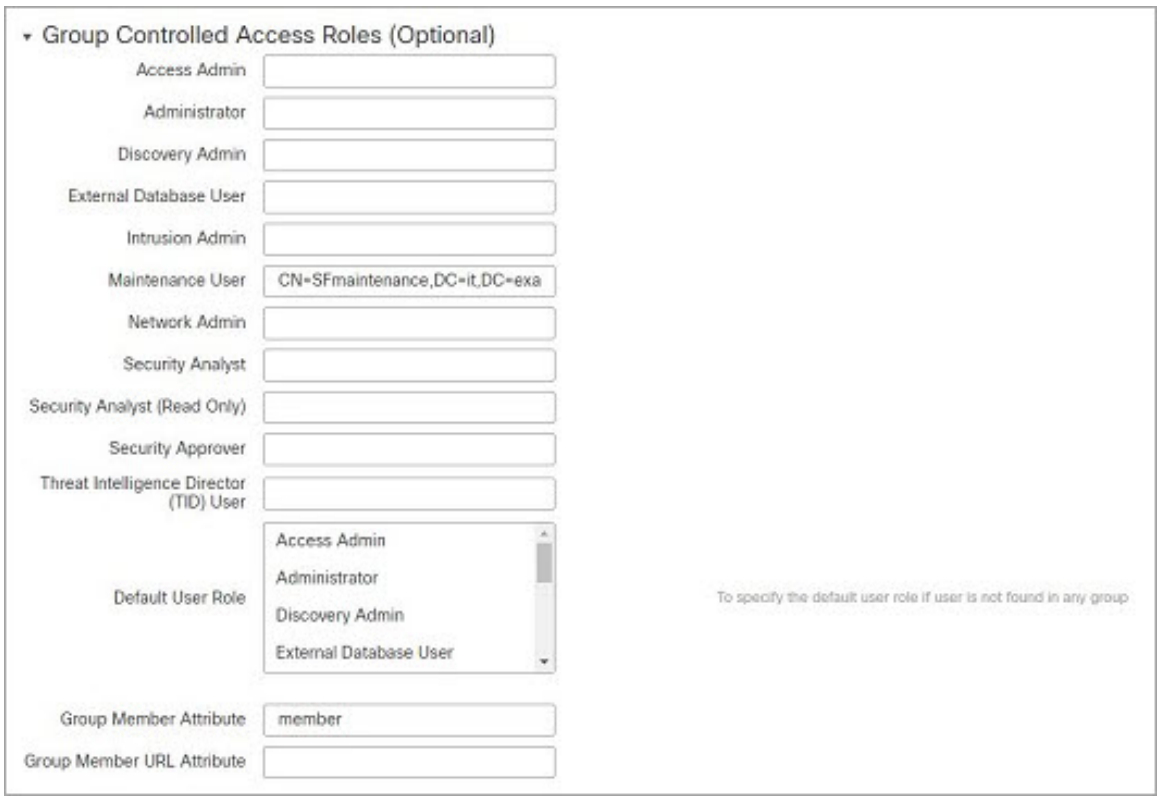


서버와의 연결은 SSL로 암호화되고 `certificate.pem`이라는 인증서가 연결에 사용됩니다. 또한 **Timeout(**시간 초과**)** 설정 때문에 60초가 지나면 서버와의 연결이 시간 초과됩니다.

이 서버는 Microsoft Active Directory Server이므로 `sAMAccountName` 속성을 사용해 사용자 이름을 저장하며 `uid` 속성을 사용하지 않습니다. 구성에 `sAMAccountName`이라는 **UI Access Attribute(UI** 액세스 속성**)**가 포함되어 있습니다. 이에 따라 시스템에서는 사용자가 시스템에 대한 로그인을 시도하는 경우 각 개체에 대해 `sAMAccountName` 속성을 검사하면서 사용자 이름을 매칭합니다.

또한 **CLI Access Attribute(CLI** 액세스 속성**)**가 `sAMAccountName`이면 사용자가 어플라이언스의 CLI 계정에 로그인할 때 디렉토리의 모든 개체에 대해 각 `sAMAccountName` 속성을 검사하여 매칭하는지 확인합니다.

여기에는 그룹 설정도 포함되어 있습니다. `member` 그룹 속성과 `CN=SFmaintenance,DC=it,DC=example,DC=com`이라는 기본 도메인 이름을 갖는 그룹의 모든 멤버에게 Maintenance User(유지 보수 사용자) 역할이 자동으로 지정됩니다.



CLI 액세스 필터는 기본 필터와 동일하게 설정되므로, 동일한 사용자가 웹 인터페이스뿐 아니라 CLI를 통해서도 어플라이언스에 액세스할 수 있습니다.

CDO에 대한 RADIUS 외부 인증 개체 추가

RADIUS 서버를 추가하고 디바이스 관리를 위해 외부 사용자를 지원합니다.

프로시저

단계 **1** 시스템 (⚙) > **Users(**사용자**)**를 선택합니다.

단계 **2** **External Authentication(**외부 인증**)**을 클릭합니다.

단계 **3** **Add External Authentication Object(**외부 인증 개체 추가**)**를 클릭합니다.

단계 **4** **Authentication Method(**인증 방법**)**을 **RADIUS**로 설정합니다.

단계 **5** **Name(**이름**)**과 **Description(**설명**)**(선택 사항)을 입력합니다.

단계 **6** **Primary Server(**기본 서버**)**에 **Host Name/IP Address(**호스트 이름**/IP** 주소**)**를 입력합니다.

단계 **7** (선택 사항) **Port(**포트**)**를 기본값에서 변경합니다.

단계 **8** **RADIUS Secret Key(RADIUS** 비밀 키**)**를 입력합니다.

단계 **9** (선택 사항) **Backup Server(**백업 서버**)** 파라미터를 입력합니다.

단계 **10** (선택 사항) **RADIUS-Specific Parameters(RADUIS** 특정 파라미터**)**를 입력합니다.

a) **Timeout(**시간 초과**)**을 초 단위(1~1024)로 입력하고 기본 서버를 다시 시도합니다. 기본값은 30입니다.

b) **Retries(**재시도**)**를 입력하고 백업 서버로 이동합니다. 기본값은 3입니다.

c) 사용자 역할에 해당하는 필드에 각 사용자의 이름을 입력하거나 해당 역할에 지정될 식별 특성-값 쌍을 입력합니다.

사용자 이름과 속성-값 쌍은 쉼표로 구분합니다.

예제**:**

보안 분석가인 모든 사용자가 `Analyst(분석가)`를 `User-Category(사용자-카테고리)` 속성 값으로 갖는 경우, `User-Category=Analyst`를 **Security Analyst(**보안 분석가 목록**)** 필드에 입력하고 해당 사용자에게 해당 역할을 부여할 수 있습니다.

예제**:**

Administrator(관리자) 역할을 사용자인`jsmith`와 `jdoe`에게 부여하려면 `jsmith, jdoe`를 **Administrator(**관리자**)** 필드에 입력합니다.

예제**:**

Maintenance User(유지 보수 사용자) 역할을 `User-Category(사용자-카테고리)` 값이 `Maintenance(유지 보수)`인 모든 사용자에게 부여하려면 `User-Category=Maintenance`를 **Maintenance User(**유지 보수 사용자**)** 필드에 입력합니다.

d) 지정된 어떤 그룹에도 속하지 않는 사용자에 대해 **Default User Role(**기본 사용자 역할**)**을 선택합니다.

사용자의 역할을 변경하는 경우, 변경된 외부 인증 개체는 저장/배포하고 **Users(**사용자**)** 화면에서 해당 사용자를 제거해야 합니다. 이 사용자는 다음 로그인 시 자동으로 재추가됩니다.

단계 **11** (선택 사항) **Define Custom RADIUS Attributes(**맞춤형 **RADIUS** 속성 정의**)**.

RADIUS 서버가 `/etc/radiusclient`의 `dictionary` 파일에 없는 속성의 값을 반환할 경우, 이러한 속성을 사용하여 해당 속성을 갖는 사용자에 대한 역할을 설정하려면 그러한 속성을 정의해야 합니다. RADIUS 서버에서 사용자 프로파일을 확인하여 사용자에 대해 반환되는 속성을 찾을 수 있습니다.

a) **Attribute Name(**속성 이름**)**을 입력합니다.

속성을 정의할 때 영숫자로 구성된 속성의 이름을 제공합니다. 속성 이름의 단어는 공백이 아닌 대시로 구분해야 합니다.

b) 정수로 **Attribute ID(**속성 **ID)**를 입력합니다.

속성 ID는 정수이며 `etc/radiusclient/dictionary` 파일에 있는 기존 속성 ID와 충돌해서는 안 됩니다.

c) **Attribute Type(**속성 유형**)** 드롭다운 목록에서 선택합니다.

속성의 유형을 문자열, IP 주소, 정수 또는 날짜로 지정합니다.

d) **Add(**추가**)**를 클릭하고 맞춤형 속성을 추가합니다.

RADIUS 인증 개체를 생성하는 경우 해당 개체에 대한 새로운 사전 파일이 `/var/sf/userauth` 디렉토리에 있는 디바이스에 생성됩니다. 추가하는 모든 맞춤형 속성은 사전 파일에 추가됩니다.

예제**:**

RADIUS 서버가 Cisco 라우터가 있는 네트워크에서 사용되는 경우 `Ascend-Assign-IP-Pool` 속성을 사용하여 특정 IP 주소 풀에서 로그인한 모든 사용자에게 특정 역할을 부여할 수 있습니다. `Ascend-Assign-IP-Pool`은 정수 속성으로서 사용자가 로그인할 수 있는 주소 풀을 정의합니다. 여기서 정수는 지정된 IP 주소 풀의 번호를 나타냅니다.

맞춤형 속성을 표시하려면 속성 이름 `Ascend-IP-Pool-Definition`, 속성 ID `218`, 속성 유형 `integer`로 맞춤형 속성을 생성합니다.

그런 다음 `Ascend-Assign-IP-Pool=2`를 **Security Analyst (Read Only)(**보안 분석가**(**읽기 전용**))** 필드에 입력하여 `Ascend-IP-Pool-Definition` 속성의 값이 `2`인 모든 사용자에게 읽기 전용 보안 분석가 권한을 부여할 수 있습니다.

단계 **12** (선택 사항) **CLI Access Filter(CLI** 액세스 필터**)** 영역 **Administrator CLI Access User List(**관리자 **CLI** 액세스 사용자 목록**)** 필드에 CLI 액세스 권한이 있어야 하는 사용자 이름을 쉼표로 구분하여 입력합니다.

이러한 사용자 이름은 RADIUS 서버의 사용자 이름과 일치해야 합니다. 이름은 다음과 같은 Linux 기준을 준수하는 사용자 이름이어야 합니다.

- 최대 32개의 영숫자 문자와 하이픈(-) 및 밑줄(_)
- 모두 소문자
- 하이픈(-)으로 시작할 수 없으며, 숫자만으로 구성할 수 없고, 마침표(.), 단가 기호(@) 또는 슬래시(/)를 포함할 수 없음

CLI 액세스에 대해 RADIUS 인증을 하지 않으려면 이 필드를 비워 둡니다.

참고 CLI 액세스 권한이 있는 사용자는 **expert** 명령을 사용하여 Linux 셸에 액세스할 수 있습니다. Linux 셸 사용자는 루트 권한을 얻을 수 있으며, 따라서 보안 위험이 발생할 수 있습니다. CLI 또는 Linux 셸 액세스 권한을 갖는 사용자의 목록을 제한해야 합니다.

참고 셸 액세스 필터에 포함된 사용자와 사용자 이름이 동일한 내부 사용자를 모두 제거합니다. management center에서는 내부 CLI 사용자만 관리자이니, 관리자 외부 사용자를 생성하지 마십시오.

단계 **13** (선택 사항) **Test(**테스트**)**를 클릭해 RADIUS 서버와 management center 연결을 테스트합니다.

단계 **14** (선택 사항) **Additional Test Parameters(**추가 테스트 파라미터**)**를 입력하고 인증 가능한 사용자의 크리덴셜을 테스트할 수 있습니다. **User Name(**사용자 이름**)** 및 **Passowrd(**비밀번호**)**를 입력한 다음 **Test(**테스트**)**를 클릭합니다.

팁 테스트 사용자의 이름이나 비밀번호를 잘못 입력할 경우 서버 구성이 맞더라도 테스트는 실패합니다. 서버 구성이 올바른지 확인하려면 먼저 **Test(**테스트**)**를 클릭합니다. 여기서 **Additional Test Parameters(**추가 테스트 파라미터**)** 필드에는 사용자 정보를 입력할 필요가 없습니다. 테스트가 성공하면 사용자 이름과 비밀번호를 입력하고 특정 사용자로 테스트하십시오.

예제**:**

예를 들어 예시 회사의 `JSmith` 사용자 크리덴셜을 가져올 수 있는지 테스트하려면 `JSmith`를 입력하고 올바른 비밀번호를 입력합니다.

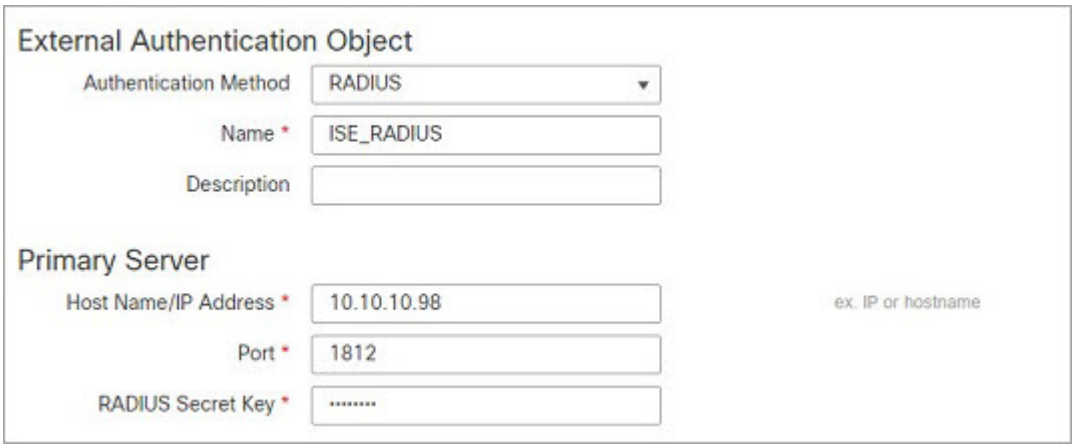
단계 **15** **Save(**저장**)**를 클릭합니다.

단계 **16** 이 서버의 사용을 활성화합니다. CDO 사용자에 대한 외부 인증 활성화, 16 페이지를 참조하십시오.

예

단순한 사용자 역할 할당

다음 그림은 포트 1812에서 IP 주소 10.10.10.98을 사용하여 Cisco ISE(Identity Services Engine)를 실행하는 서버를 위한 RADIUS 로그인 인증 개체의 예를 보여줍니다. 정의된 백업 서버가 없습니다.



다음 예는 RADIUS 관련 매개변수를 보여줍니다. 여기에는 시간 초과(30초) 및 Firepower System이 백업 서버에 연결을 시도하기 전 실패한 재시도 횟수(있는 경우)가 포함됩니다.

이 예에서는 RADIUS 사용자 역할 구성의 주요 측면을 보여줍니다.

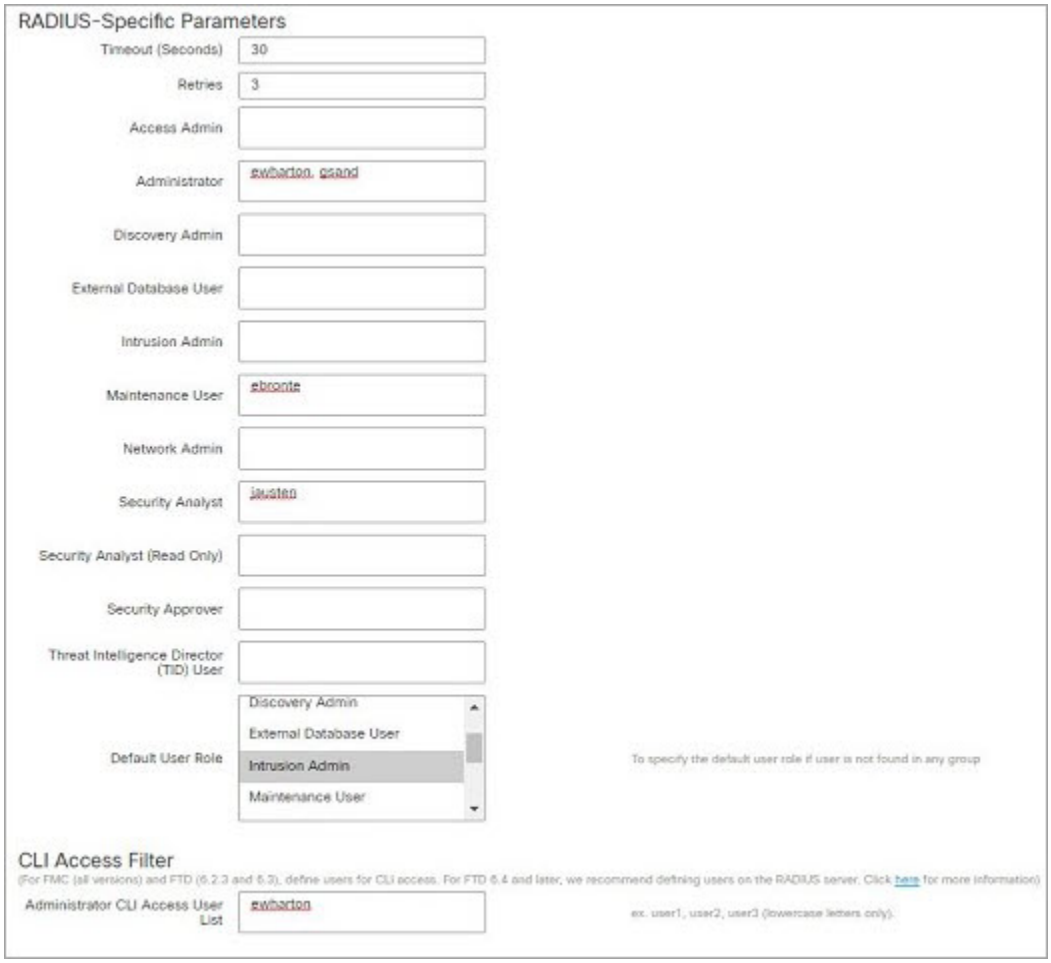
사용자 `ewharton` 및 `gsand`에게 웹 인터페이스 Administrator(관리자) 액세스 권한이 주어집니다.

사용자 cbronte에게 웹 인터페이스 Maintenance User(유지 보수 사용자) 액세스 권한이 주어집니다.

사용자 jausten에게 웹 인터페이스 Security Analyst(보안 분석가) 액세스 권한이 주어집니다.

사용자 ewharton은 CLI 계정을 사용하여 디바이스에 로그인할 수 있습니다.

다음 그림은 이 예시에서의 역할 구성을 나타냅니다.



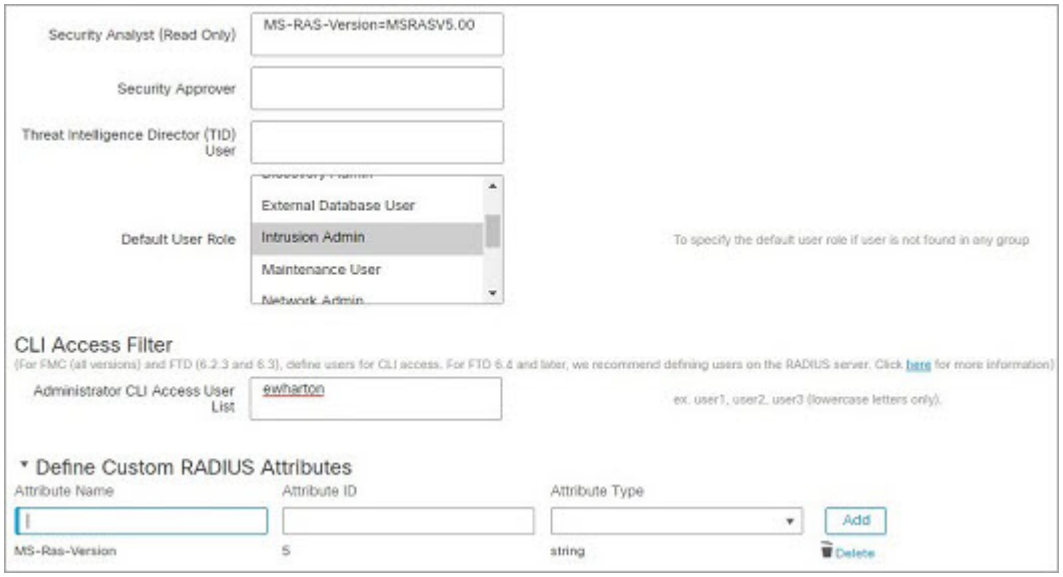
속성-값 쌍을 매칭하는 사용자의 역할

속성-값 쌍을 사용하여 특정 사용자 역할을 갖는 사용자를 식별할 수 있습니다. 사용하는 속성이 맞춤형 속성일 경우 해당 맞춤형 속성을 정의해야 합니다.

다음 그림은 이전의 예와 동일한 ISE 서버를 위한 샘플 RADIUS 로그인 인증 개체에 포함된 역할 설정 및 맞춤형 속성 정의를 보여줍니다.

그러나 여기서는 Microsoft 원격 액세스 서버가 사용 중이므로 MS-RAS-Version 맞춤형 속성 한 명 이상의 사용자에게 반환됩니다. 참고로 MS-RAS-Version 맞춤형 속성은 문자열입니다. 이 예에서는 Microsoft v. 5.00 원격 액세스 서버를 통해 RADIUS로 로그인하는 모든 사용자가 Security Analyst(Read Only)(보안 분석가(읽기 전용)) 역할을 받아야 하므로 속성-값 쌍

`MS-RAS-Version= MSRASV5.00`을 **Security Analyst(Read Only)(**보안 분석가**(**읽기 전용**))** 필드에 입력합니다.



CDO 사용자에 대한 외부 인증 활성화

관리 사용자에 대한 외부 인증을 활성화하는 경우, External Authentication(외부 인증) 개체에 지정된 대로 management center이 LDAP 또는 RADIUS 서버로 사용자 크리덴셜을 확인합니다.

시작하기 전에

CDO에 대한 LDAP 외부 인증 개체 추가, 4 페이지 및 CDO에 대한 RADIUS 외부 인증 개체 추가, 11 페이지에 따라 외부 인증 개체를 1개 이상 추가합니다.

프로시저

단계 **1** 시스템 (⚙) > **Users(**사용자**)**를 선택합니다.

단계 **2** **External Authentication(**외부 인증**)**을 클릭합니다.

단계 **3** 외부 웹 인터페이스 사용자에 대한 기본 사용자 역할을 설정합니다.

역할이 없는 사용자가 어떤 작업도 수행할 수 없습니다. 외부 인증 개체에 정의된 사용자 역할이 이 기본 사용자 역할보다 우선합니다.

a) **Default User Roles(**기본 사용자 역할**)** 값을 클릭합니다(기본적으로 none(해당 없음) 선택됨).

a) **Default User Role Configuration(**기본 사용자 역할 구성**)** 대화 상자에서 사용하려는 역할(복수 가능)을 선택합니다.

b) **Save(**저장**)**를 클릭합니다.

단계 **4** 사용하려는 각 외부 인증 개체 옆 **Slider enabled(**슬라이더 활성화됨**)** ( )를 클릭합니다. 개체를 1개 이상 활성화하는 경우, 사용자가 지정된 순서대로 서버와 비교됩니다. 다음 단계를 참조하고 서버를 재정렬합니다.

셸 인증을 활성화하는 경우에 **CLI** 액세스 필터를 포함하는 외부 인증 개체를 활성화해야 합니다. 또한 CLI 액세스 사용자는 인증 개체가 목록에서 순위가 가장 높은 서버에 대해서만 인증할 수 있습니다.

단계 **5** (선택 사항) 인증 요청이 발생한 경우 서버를 드래그 앤 드롭하고 인증 순서를 변경합니다.

단계 **6** 외부 사용자에 대해 CLI 액세스를 허용하려면, **Shell Authentication(**셸 인증**)** > **Enabled(**활성화**)**를 선택합니다.

첫 번째 외부 인증 개체 이름이 **Enabled(**활성화**)** 옵션 옆에 표시되고 첫 번째 개체만 CLI 액세스에 사용된다고 알립니다.

단계 **7** **Save and Apply(**저장 및 적용**)**를 클릭합니다.

LDAP 인증 연결 문제 해결

LDAP 인증 개체를 생성하는 경우, 선택한 서버와의 연결에 실패하거나 원하는 사용자 목록을 가져오지 않는다면 개체의 설정을 조정할 수 있습니다.

연결 테스트 결과 연결에 실패할 경우, 다음 방법으로 구성 문제를 해결해보십시오.

- 웹 인터페이스 화면 상단 및 테스트 출력에 표시된 메시지를 참조하여 개체의 어느 영역에서 문제를 일으키는지 확인합니다.
- 개체에 사용한 사용자 이름과 비밀번호가 올바른지 확인합니다.
  - 사용자가 기본 DN에 나타난 디렉토리로 이동할 권한이 있는지 확인하기 위해 서드파티 LDAP 브라우저를 사용하여 LDAP 서버에 연결해봅니다.
  - 사용자 이름이 LDAP 서버의 디렉토리 정보 트리에서 고유한지 확인합니다.
  - 테스트 출력에 LDAP 바인드 오류 49가 있을 경우 해당 사용자에 대한 사용자 바인딩이 실패한 것입니다. 서드파티 애플리케이션을 통해 서버 인증을 시도하여 해당 연결에서도 바인딩이 실패하는지 확인합니다.
- 서버를 정확하게 식별했는지 확인합니다.
  - 서버 IP 주소 또는 호스트 이름이 정확한지 확인합니다.
  - 로컬 어플라이언스에서 연결할 인증 서버까지 TCP/IP 액세스 권한이 있는지 확인합니다.
  - 서버에 대한 액세스가 방화벽에 의해 차단되지 않고 개체에 구성한 포트가 열려 있는지 확인합니다.
  - TLS 또는 SSL을 통한 연결에 인증서를 사용하는 경우 인증서의 호스트 이름이 서버에 사용된 호스트 이름과 일치해야 합니다.

  - CLI 액세스를 인증하는 경우, 서버 연결에 IPv6 주소를 사용하지 않았는지 확인합니다.
  - 서버 유형 기본값을 사용한 경우 정확한 서버 유형인지 확인하고 **Set Defaults(**기본값 설정**)**를 다시 클릭하여 기본값을 재설정합니다.

- 기본 DN을 입력한 경우 **Fetch DNs(DN** 가져오기**)**를 클릭하여 서버에서 사용 가능한 모든 기본 DN을 가져오고 그 목록에서 이름을 선택합니다.
- 필터, 액세스 특성 또는 고급 설정을 사용하는 경우 각각이 올바르고 제대로 입력되었는지 확인합니다.
- 필터, 액세스 특성 또는 고급 설정을 사용하는 경우 각 설정을 제거하고 그 설정 없이 개체를 테스트해봅니다.
- 기본 필터 또는 CLI 액세스 필터를 사용하는 경우, 필터가 괄호로 묶여 있고 올바른 비교 연산자를 사용하고 있는지 확인합니다. 묶인 괄호를 포함하여 최대 450자까지 입력할 수 있습니다.
- 더 제한적인 기본 필터를 테스트하려면 사용자의 기본 DN으로 설정하여 그 사용자만 검색해봅니다.
- 암호화 연결을 사용하는 경우:
  - 인증서에 있는 LDAP 서버의 이름이 연결에 사용하는 호스트 이름과 매칭되는지 확인합니다.
  - 암호화 서버 연결에 IPv6 주소를 사용하지 않았는지 확인합니다.
- 테스트 사용자를 사용하는 경우 사용자 이름과 비밀번호가 제대로 입력되었는지 확인합니다.
- 테스트 사용자를 사용하는 경우 사용자 크리덴셜을 제거하고 개체를 테스트합니다.
- LDAP 서버에 연결하고 다음 구문을 사용하여 사용 중인 쿼리를 테스트합니다.

```
ldapsearch -x -b 'base_distinguished_name'
-h LDAPserver_ip_address -p port -v -D
'user_distinguished_name' -W 'base_filter'
```

  예를 들어 `myrtle.example.com`의 보안 도메인에 연결하기 위해 `domainadmin@myrtle.example.com` 사용자와 (`cn=*`) 기본 필터를 사용하는 경우, 다음 구문으로 연결을 테스트할 수 있습니다.

```
ldapsearch -x -b 'CN=security,DC=myrtle,DC=example,DC=com'
-h myrtle.example.com -p 389 -v -D
'domainadmin@myrtle.example.com' -W '(cn=*)'
```

연결 테스트에 성공했지만 플랫폼 설정 정책을 적용한 후 인증이 되지 않을 경우, 디바이스에 적용되는 플랫폼 설정 정책에서 인증 및 사용할 개체가 모두 활성화되었는지 확인합니다.

성공적으로 연결했지만 연결에서 검색되는 사용자 목록을 조정하려는 경우, 기본 필터 또는 CLI 액세스 필터를 추가하거나 변경할 수 있습니다. 또는 더 제한적이거나 덜 제한적인 기본 DN을 사용할 수 있습니다.

AD(Active Directory) 서버에 대한 연결을 인증하는 동안에는 AD 서버에 대한 연결에 성공하더라도 연결 이벤트 로그에 차단된 LDAP 트래픽이 표시되는 경우가 거의 없습니다. 이 잘못된 연결 로그는 AD 서버가 중복 재설정 패킷을 전송할 때 발생합니다. Threat Defense 디바이스는 두 번째 재설정 패킷을 새 연결 요청의 일부로 식별하고 Block(차단) 작업으로 연결을 로깅합니다.