ID 소스

ID 소스는 사용자 어카운트를 정의하는 서버와 데이터베이스입니다. 이 정보는 IP 주소와 연결된 사용자 ID를 제공하거나, 원격 액세스 VPN 연결 또는 device manager 액세스를 인증하는 등 다양한 방식으로 사용할 수 있습니다.

다음 주제에서는 ID 소스를 정의하는 방법을 설명합니다. 그런 다음, ID 소스가 필요한 서비스를 구성할 때 이러한 개체를 사용할 수 있습니다.

ID 소스 정보

ID 소스는 조직 내 사용자의 사용자 어카운트를 정의하는 AAA 서버와 데이터베이스입니다. 이 정보는 IP 주소와 연결된 사용자 ID를 제공하거나, 원격 액세스 VPN 연결 또는 device manager 액세스를 인증하는 등 다양한 방식으로 사용할 수 있습니다.

Objects(개체**)** > **Identity Sources(ID** 소스**)** 페이지에서 소스를 생성하고 관리합니다. 그런 다음, ID 소스가 필요한 서비스를 구성할 때 이러한 개체를 사용할 수 있습니다.

지원되는 ID 소스와 사용 방법은 다음과 같습니다.

AD(Active Directory) ID 영역

Active Directory에서 사용자 어카운트 및 인증 정보를 제공합니다. AD(Active Directory) ID 영역, 3 페이지의 내용을 참조하십시오.

이 소스는 다음과 같은 목적으로 사용할 수 있습니다.

- 원격 액세스 VPN(기본 ID 소스로 사용) AD를 RADIUS 서버와 함께 사용할 수 있습니다.
- ID 정책(활성 인증용으로 사용/패시브 인증에 사용되는 사용자 ID 소스로 사용)

AD(Active Directory) 영역 시퀀스

AD 영역 시퀀스는 AD 영역 개체의 순서가 지정된 목록입니다. 영역 시퀀스는 네트워크에서 두 개 이상의 AD 도메인을 관리하는 경우 유용합니다. AD 영역 시퀀스 구성하기, 7 페이지의 내용을 참조하십시오.

이 소스는 다음과 같은 목적으로 사용할 수 있습니다.

- ID 정책(패시브 인증에 사용되는 사용자 ID 소스로 사용) 시퀀스에서 영역의 순서는 시스템에서 드물게 충돌이 발생하는 경우 사용자 ID를 결정하는 방식을 결정합니다.

Cisco ISE(Identity Services Engine) 또는 **Cisco ISE PIC(Identity Services Engine Passive Identity Connector)**

ISE를 사용하는 경우 위협 방어 디바이스를 ISE 구축과 통합할 수 있습니다. Identity Services Engine (ISE), 14 페이지의 내용을 참조하십시오.

이 소스는 다음과 같은 목적으로 사용할 수 있습니다.

- ID 정책(ISE에서 사용자 ID를 수집하기 위한 패시브 ID 소스로 사용)

RADIUS 서버**, RADIUS** 서버 그룹

RADIUS 서버를 사용하는 경우 device manager와 함께 사용할 수도 있습니다. 각 서버를 별도의 개체로 정의한 후에 서버 그룹에 포함할 수 있습니다. 여기서 지정된 그룹의 서버는 서로의 복사본입니다. 개별 서버가 아닌 서버 그룹을 기능에 할당해야 합니다. RADIUS 서버 및 그룹, 10 페이지의 내용을 참조하십시오.

이 소스는 다음과 같은 목적으로 사용할 수 있습니다.

- 인증용 ID 소스이자 권한 부여 및 과금 용도의 원격 액세스 VPN. AD를 RADIUS 서버와 함께 사용할 수 있습니다.
- ID 정책(원격 액세스 VPN 로그인에서 사용자 ID를 수집하기 위한 패시브 ID 소스로 사용)
- device manager 또는 위협 방어 CLI 관리 사용자에 대한 외부 인증. 인증 레벨이 각기 다른 여러 관리 사용자를 지원할 수 있습니다. 이 사용자는 디바이스 컨피그레이션 및 모니터링을 위해 시스템에 로그인할 수 있습니다.

SAML 서버

SAML 2.0(Security Assertion Markup Language 2.0)은 당사자 간에 인증 및 권한 부여 데이터, 특히 IdP(Identity Provider)와 SP(Service Provider)를 교환하기 위한 개방형 표준입니다.

이 소스는 다음과 같은 목적으로 사용할 수 있습니다.

- SSO(Single Sign-On) 인증 소스로서의 원격 액세스 VPN.

로컬 **ID** 소스

device manager에서 정의한 사용자를 포함하는 로컬 사용자 데이터베이스입니다. 이 데이터베이스에서 사용자 어카운트를 관리하려면 **Objects(**개체**)** > **Users(**사용자**)**를 선택합니다. 로컬 사용자, 20 페이지의 내용을 참조하십시오.

참고 로컬 ID 소스 데이터베이스에는 CLI 액세스를 위해 **configure user add** 명령을 사용하여 CLI에서 구성한 사용자는 포함되지 않습니다. CLI 사용자는 device manager에서 생성하는 사용자와는 완전히 별개의 사용자입니다.

이 소스는 다음과 같은 목적으로 사용할 수 있습니다.

- 원격 액세스 VPN(기본 또는 대체 ID 소스로 사용)
- ID 정책(원격 액세스 VPN 로그인에서 사용자 ID를 수집하기 위한 패시브 ID 소스로 사용)

AD(Active Directory) ID 영역

Microsoft AD(Active Directory)는 사용자 어카운트를 정의합니다. Active Directory 도메인의 AD ID 영역을 생성할 수 있습니다. 다음 주제에서는 AD ID 영역을 정의하는 방법을 설명합니다.

지원되는 디렉터리 서버

Windows Server 2012, 2016, 및 2019에서 Microsoft AD(Active Directory)를 사용할 수 있습니다.

서버 컨피그레이션과 관련하여 다음 사항에 유의하십시오.

- 사용자 그룹 또는 그룹 내의 사용자에 대해 사용자 제어를 수행하려면 디렉터리 서버에서 사용자 그룹을 구성해야 합니다. 서버가 기본 개체 계층으로 사용자를 구성하는 경우 시스템은 사용자 그룹 제어를 수행할 수 없습니다.
- 디렉터리 서버는 시스템에 대해 다음 표에 나와 있는 필드 이름을 순서대로 사용하여 해당 필드에 대한 사용자 메타데이터를 서버에서 검색해야 합니다.

메타데이터	**Active Directory Field(Active Directory** 필드**)**
LDAP user name(LDAP 사용자 이름)	samaccountname
first name(이름)	givenname
last name(성)	sn
email address(이메일 주소)	mail userprincipalname(메일에 값이 없는 경우)
department(부서)	department distinguishedname(부서에 값이 없는 경우)
telephone number(전화번호)	telephonenumber

사용자 수 제한사항

Device Manager는 디렉터리 서버에서 최대 50,000명의 사용자에 대한 정보를 다운로드할 수 있습니다.

디렉터리 서버에 50,000개가 넘는 사용자 계정이 포함되어 있으면 액세스 규칙에서 사용자를 선택할 때 또는 사용자 기반 대시보드 정보를 확인할 때 가능한 이름이 모두 표시되지 않으며, 다운로드한 이름에 대해서만 규칙을 작성할 수 있습니다.

이 제한은 그룹과 연결된 이름에도 적용됩니다. 그룹의 구성원이 50,000명보다 많으면 다운로드한 50,000개의 이름에 대해서만 그룹 구성원 자격과의 일치 여부를 확인할 수 있습니다.

디렉터리 기본 **DN** 결정

디렉터리 속성을 구성할 때는 사용자와 그룹에 대한 공통 기본 DN(고유 이름)을 지정해야 합니다. 이 기준은 디렉터리 서버에서 정의되며 네트워크마다 다릅니다. 올바른 기준을 입력해야 ID 정책이 실행됩니다. 기준이 잘못된 경우 시스템이 사용자 또는 그룹 이름을 확인할 수 없으므로 ID 기반 정책이 실행될 수 없습니다.

팁 올바른 기준을 가져오려면 디렉터리 서버 담당 관리자에게 문의하십시오.

Active Directory의 경우, 도메인 관리자로 Active Directory 서버에 로그인하여 다음과 같이 명령 프롬프트에 **dsquery** 명령을 사용해 기준을 확인하여 올바른 기준을 확인할 수 있습니다.

사용자 검색 기준

알려진 사용자 이름(부분 또는 전체)을 포함한 **dsquery user** 명령을 입력하여 기본 고유 이름을 확인합니다. 예를 들어, 다음 명령은 부분 이름 "John*"를 사용하여 "John"으로 시작되는 모든 사용자에 대한 정보를 반환합니다.

```
C:\Users\Administrator>dsquery user -name "John*"
"CN=John Doe,CN=Users,DC=csc-lab,DC=example,DC=com"
```

이 경우 기본 DN은 "DC=csc-lab,DC=example,DC=com"이 됩니다.

그룹 검색 기준

알려진 그룹 이름을 포함한 **dsquery group** 명령을 입력하여 기본 고유 이름을 확인합니다. 예를 들어, 다음 명령은 그룹 이름 Employees를 사용하여 고유 이름을 반환합니다.

```
C:\>dsquery group -name "Employees"
"CN=Employees,CN=Users,DC=csc-lab,DC=example,DC=com"
```

이 경우 그룹 기본 DN은 "DC=csc-lab,DC=example,DC=com"이 됩니다.

ADSI 수정 프로그램을 사용하여 Active Directory 구조를 찾을 수도 있습니다(**Start(**시작**)** > **Run(**실행**)** > **adsiedit.msc**). ADSI 편집에서 조직 단위(OU), 그룹, 사용자 등의 개체를 마우스 오른쪽 단추로

클릭하고 **Properties(**속성**)**를 선택하여 고유 이름을 확인합니다. 그러면 DC 값 문자열을 기준으로 복사할 수 있습니다.

기준이 올바른지를 확인하려면 다음 단계를 수행합니다.

1. 디렉터리 속성의 Test Connection(연결 테스트) 버튼을 클릭하여 연결을 확인합니다. 모든 문제를 해결하고 디렉터리 속성을 저장합니다.
2. 디바이스에 변경 사항을 커밋합니다.
3. 액세스 규칙을 생성하고 **Users(**사용자**)** 탭을 선택한 다음 디렉터리에서 알려진 사용자 및 그룹 이름을 추가해 봅니다. 디렉터리가 포함된 영역에서 일치하는 사용자 및 그룹을 입력하면 자동 완성 제안 사항이 표시됩니다. 이러한 제안 사항이 드롭다운 목록에 표시되는 경우 시스템이 디렉터리를 정상적으로 쿼리한 것입니다. 입력한 문자열이 사용자 또는 그룹 이름에 포함되어 있는데 제안 사항이 표시되지 않으면 해당하는 검색 기준을 편집해야 합니다.

AD ID 영역 구성

ID 영역은 디렉터리 서버와 인증 서비스를 제공하는 데 필요한 기타 특성입니다. 디렉터리 서버는 네트워크 액세스가 허용되는 사용자 및 사용자 그룹에 대한 정보를 포함합니다.

Active Directory의 경우 영역은 Active Directory 도메인과 동일합니다. 지원해야 하는 각 AD 도메인에 대해 별도 영역을 생성합니다.

영역은 다음 정책에서 사용됩니다.

- ID - 영역은 사용자 ID 및 그룹 멤버십 정보를 제공합니다. 액세스 제어 규칙에서 이러한 정보를 사용할 수 있습니다. 시스템은 매일 마지막 시간(UTC)에 모든 사용자와 그룹에 대한 업데이트된 정보를 다운로드합니다. 디렉터리 서버는 관리 인터페이스에서 연결 가능해야 합니다.
- 원격 액세스 VPN — 영역은 연결 허용 여부를 결정하는 인증 서비스를 제공합니다. 디렉터리 서버는 RA VPN 외부 인터페이스에서에서 연결 가능해야 합니다.
- 액세스 제어, SSL 암호 해독 — 규칙의 사용자 기준에서 영역을 선택하여 이 규칙을 영역 내 모든 사용자에게 적용할 수 있습니다.

디렉터리 관리자와 협의하여 디렉터리 서버 속성을 구성하는 데 필요한 값을 가져오십시오.

참고 디렉터리 서버가 연결된 네트워크에 있지 않거나 기본 경로를 통해 사용할 수 없는 상태이면 서버에 대해 정적 경로를 생성합니다. **Device(**디바이스**)** > **Routing(**라우팅**)** > **View Configuration(**설정 보기**)**을 선택하여 정적 경로를 생성합니다.

다음 절차에서는 개체 페이지를 통해 개체를 직접 생성하고 수정할 수 있는 방법을 설명합니다. 개체 목록에 표시되는 새 **ID** 영역 생성 링크를 클릭하여 영역 속성을 수정하면서 ID 영역 개체를 생성할 수도 있습니다.

시작하기 전에

디렉터리 서버, threat defense 디바이스 및 클라이언트에서 시간 설정이 서로 일치하는지 확인합니다. 이러한 디바이스 간에 시간이 바뀌면 사용자가 정상적으로 인증하지 못할 수 있습니다. 여기서 "일치"란 여러 표준 시간대를 사용할 수는 있지만 이러한 표준 시간대를 기준으로 할 때 시간이 동일해야 한다는 의미입니다. 예를 들어 PST로 오전 10시는 EST로 오후 1시에 해당합니다.

프로시저

단계 **1** 목차에서 **Objects(**개체**)**와 **Identity Sources(ID** 소스**)**를 차례로 선택합니다.

단계 **2** 다음 중 하나를 수행합니다.

- AD 영역을 생성하려면 **+** > **AD**를 클릭합니다.
- 영역을 수정하려면 해당 영역의 수정 아이콘()을 클릭합니다.

참조되지 않는 개체를 삭제하려면 해당 개체의 휴지통 아이콘()을 클릭합니다.

단계 **3** 기본 영역 속성을 구성합니다.

- **Name(**이름**)** - 디렉토리 영역의 이름입니다.
- **Type(**유형**)** - 디렉터리 서버의 유형입니다. 지원되는 유형은 Active Directory뿐이며 이 필드의 내용은 변경할 수 없습니다.
- **Directory Username(**디렉터리 사용자 이름**)**, **Directory Password(**디렉터리 비밀번호**)** - 검색하려는 사용자 정보에 대한 적절한 권한이 있는 사용자의 고유 사용자 이름 및 비밀번호입니다. Active Directory의 경우에는 사용자에게 상승된 권한이 필요하지 않습니다. 도메인에 어떤 사용자라도 지정할 수 있습니다. 사용자 이름은 모든 자격 요건에 부합해야 합니다(예: 단지 Administrator가 아닌 Administrator@example.com).

  참고 시스템은 이 정보에서 ldap-login-dn 및 ldap-login-password를 생성합니다. 예를 들어 Administrator@example.com은 cn=administrator,cn=users,dc=example,dc=com으로 변환됩니다. cn=users는 항상 이 변환에 포함되므로 일반 이름 "users" 폴더 아래에 여기서 지정하는 사용자를 구성해야 합니다.

- **Base DN(**기본 **DN)** - 사용자 및 그룹 정보를 검색하거나 쿼리하기 위한 디렉터리 트리, 즉 사용자와 그룹의 공통 상위 항목입니다. cn=users,dc=example,dc=com을 예로 들 수 있습니다. 기본 DN을 찾는 방법에 대한 자세한 내용은 디렉터리 기본 DN 결정, 4 페이지를 참조하십시오.
- **AD Primary Domain(AD** 기본 도메인**)** - 디바이스가 조인해야 하는 정규화된 Active Directory 도메인 이름입니다. example.com 등을 예로 들 수 있습니다.

단계 **4** 디렉터리 서버 속성을 구성합니다.

- **Hostname/IP Address(**호스트 이름**/IP** 주소**)** - 디렉터리 서버의 호스트 이름 또는 IP 주소입니다. 서버에 대한 암호화된 연결을 사용하는 경우에는 IP 주소가 아닌 FQDN(Fully-Qualified Domain Name)을 입력해야 합니다.

- **Port(포트)** - 서버와의 통신에 사용되는 포트 번호입니다. 기본값은 389입니다. 암호화 방법으로 LDAPS를 선택하는 경우에는 포트 636을 사용합니다.
- **Encryption(암호화)** - 사용자 및 그룹 정보를 다운로드하기 위해 암호화된 연결을 사용하려는 경우에는 **STARTTLS** 또는 **LDAPS** 중에서 원하는 방법을 선택합니다. 기본값은 **None(없음)**입니다. 이 옵션은 사용자 및 그룹 정보를 일반 텍스트로 다운로드함을 의미합니다.
  - **STARTTLS**는 암호화 방법을 협상하여 디렉토리 서버가 지원하는 가장 강력한 방법을 사용하며 포트 389를 사용합니다. 원격 액세스 VPN에 영역을 사용하는 경우에는 이 옵션이 지원되지 않습니다.
  - **LDAPS**를 선택하는 경우 LDAP over SSL이 필요합니다. 이 옵션은 포트 636을 사용합니다.
- **Trusted CA Certificate(신뢰할 수 있는 CA 인증서)** - 암호화 방법을 선택하는 경우 CA(인증 증명) 인증서를 업로드하여 시스템과 디렉터리 서버 간에 신뢰할 수 있는 연결을 설정합니다. 인증서를 사용하여 인증하는 경우에는 인증서의 서버 이름이 서버 호스트 이름/IP 주소와 일치해야 합니다. 예를 들어 IP 주소로 10.10.10.250을 사용하는데 인증서의 주소는 ad.example.com이면 연결은 실패합니다.

단계 **5** 해당 영역에 여러 개의 서버가 있는 경우, **Add Another Configuration(다른 컨피그레이션 추가)**을 클릭하고 각 추가 서버에 대해 속성을 입력합니다.

해당 영역에 최대 10개의 AD 서버를 추가할 수 있습니다. 이 서버들은 서로의 중복이어야 하고 동일한 AD 도메인을 지원해야 합니다.

편의에 따라 각 서버 항목을 축소 및 확장할 수 있습니다. 섹션에는 호스트네임/IP 주소 및 포트로 레이블이 지정됩니다.

단계 **6** **Test(테스트)** 버튼을 클릭하여 시스템이 서버에 연결할 수 있는지 확인합니다.

시스템은 별도의 프로세스와 인터페이스를 사용하여 서버에 액세스하므로, 연결이 특정 사용 유형에는 작동하지만 다른 유형에는 작동하지 않음을 나타내는 오류가 발생합니다. 연결을 ID 정책에는 사용할 수 있지만, 원격 액세스 VPN에는 사용할 수 없는 경우를 예로 들 수 있습니다. 서버에 연결할 수 없는 경우에는 IP 주소와 호스트 이름이 올바른지와 DNS 서버에 호스트 이름의 항목이 있는지 등을 확인합니다. 서버에 대한 정적 경로를 구성해야 할 수 있습니다. 자세한 내용은 디렉터리 서버 연결 트러블슈팅, 8 페이지를 참고하십시오.

단계 **7** **OK(확인)**를 클릭합니다.

AD 영역 시퀀스 구성하기

패시브 ID 규칙에서 AD 영역 시퀀스를 사용하여 시스템이 둘 이상의 AD 서버에서 사용자를 일치시키려고 시도할 수 있습니다. 영역 시퀀스에서는 각 AD 서버가 다른 영역 또는 도메인(예: engineering.example.com 및 marketing.example.com)을 관리하는 AD 영역의 순서가 지정된 목록을 구성합니다.

영역 시퀀스는 두 개 이상의 AD 도메인을 지원하고, 다른 도메인의 사용자가 threat defense 디바이스를 통해 트래픽을 전송할 수 있는 경우에만 유용합니다. 영역은 소극적으로 인증된 사용자 세션에 대

한 ID를 찾기 위해 사용됩니다. 이 영역의 순서는 충돌이 발생할 수 있는 드문 경우를 비롯하여 ID 충돌을 해결하는 데 사용됩니다.

프로시저

단계 **1** 목차에서 **Objects(**개체**)**와 **Identity Sources(ID** 소스**)**를 차례로 선택합니다.

단계 **2** 다음 중 하나를 수행합니다.

- AD 영역 시퀀스를 생성하려면 **+** > **AD** 영역 시퀀스를 클릭합니다.
- AD 영역 시퀀스를 수정하려면 개체의 edit icon(수정 아이콘)()을 클릭하십시오.

참조되지 않는 개체를 삭제하려면 해당 개체의 휴지통 아이콘()을 클릭합니다.

단계 **3** 영역 시퀀스 속성을 구성합니다:

- **Name(**이름**)** - 개체의 이름입니다.
- **Description(**설명**)** - 개체의 설명(선택 사항)입니다.
- **AD Realms(AD** 영역**)** — AD 영역 개체를 시퀀스에 추가하려면 **+**를 클릭합니다. 영역을 추가한 후에는 원하는 순서가 지정된 시퀀스로 영역을 클릭하여 끌어다 놓습니다.

단계 **4** **OK(**확인**)**를 클릭합니다.

이제 패시브 ID 규칙에서 AD 영역 시퀀스를 선택할 수 있습니다.

디렉터리 서버 연결 트러블슈팅

시스템은 디렉터리 서버와 통신하기 위해 기능에 따라 다양한 프로세스를 사용합니다. 따라서, ID 정책에 대한 연결은 성공하는 반면 원격 액세스 VPN에 대한 연결에는 실패할 수 있습니다.

이러한 프로세스는 각기 다른 인터페이스를 사용하여 디렉터리 서버와 통신합니다. 다음 인터페이스에서의 연결을 확인해야 합니다.

- ID 정책용 관리 인터페이스.
- 원격 액세스 VPN용 데이터 인터페이스(외부 인터페이스).

ID 영역을 구성할 때 연결에 성공할 수 있는지 확인하기 위해 **Test(**테스트**)** 버튼을 사용합니다. 실패 메시지는 연결에 문제가 있는 기능을 나타냅니다. 다음은 인증 특성 및 라우팅/인터페이스 컨피그레이션에 따라 사용자가 접할 수 있는 일반적인 문제입니다.

디렉터리 사용자 인증 문제입니다**.**

사용자 이름 또는 비밀번호로 인해 시스템이 디렉터리 서버에 로그인할 수 없는 문제의 경우, 이름 및 비밀번호가 디렉터리 서버에 대해 정확하고 유효한지 확인하십시오. Active Directory의 경우에는 사용자에게 상승된 권한이 필요하지 않습니다. 도메인에 어떤 사용자라도 지정할 수 있

습니다. 사용자 이름은 모든 자격 요건에 부합해야 합니다(예: 단지 Administrator가 아닌 Administrator@example.com).

시스템은 사용자 이름 및 비밀번호 정보에서 ldap-login-dn 및 ldap-login-password를 생성합니다. 예를 들어 Administrator@example.com은 cn=administrator,cn=users,dc=example,dc=com으로 변환됩니다. cn=users는 항상 이 변환의 일부이므로 여기에서 일반 이름 "users" 폴더 아래에 지정하는 사용자를 구성해야 합니다.

디렉터리 서버에는 데이터 인터페이스를 통해 액세스할 수 있습니다.

디렉터리 서버가 데이터 인터페이스(예: GigabitEthernet 인터페이스)에 직접 연결된 네트워크에 있거나 직접 연결된 네트워크에서 라우팅 가능한 경우, 가상 관리 인터페이스 및 디렉터리 서버 간에 경로가 있는지 확인해야 합니다.

- **data-interfaces**를 관리 게이트웨이로 사용할 경우, 라우팅에 성공해야 합니다.
- 관리 인터페이스에 명시적 게이트웨이가 있는 경우, 해당 게이트웨이 라우터는 디렉터리 서버에 대한 경로를 갖고 있어야 합니다.
- 가상 관리 인터페이스에서 사용하는 실제 인터페이스인 진단 인터페이스에서 IP 주소를 구성할 필요가 없습니다. 그러나 주소를 구성하는 경우 디렉터리 서버에 대한 트래픽을 진단 인터페이스로 리디렉션하는 정적 경로(예: 기본 경로)를 구성하지 마십시오.
- 직접 연결된 네트워크와 디렉터리 서버를 호스팅하는 네트워크 사이에 라우터가 있는 경우, 디렉터리 서버에 대한 정적 경로를 구성합니다(**Device(**디바이스**)** > **Routing(**라우팅**)**).
- 데이터 인터페이스에 올바른 IP 주소 및 서브넷 마스크가 있는지 확인합니다.

디렉터리 서버에는 관리 실제 인터페이스를 통해 액세스할 수 있습니다.

디렉터리 서버가 관리 실제 인터페이스(예: Management0/0)에 직접 연결된 네트워크에 있거나 해당 네트워크에서 라우팅 가능한 경우, 다음 작업을 수행해야 합니다.

- **Device(**디바이스**)** > **Interfaces(**인터페이스**)**에서 관리 인터페이스(논리적 이름이 진단)의 IPv4 주소를 설정합니다. IP 주소는 가상 관리 주소(**Device(**디바이스**)** > **System Settings(**시스템 설정**)** > **Management Interface(**관리 인터페이스**)**)와 동일한 서브넷에 있어야 합니다.
- 디렉터리 서버와 관리 인터페이스 사이에 라우터가 있는 경우, 진단 인터페이스에 대해 **Device(**디바이스**)** > **Routing(**라우팅**)**에서 디렉터리 서버의 경로를 설정합니다.
- 진단 인터페이스와 관리 인터페이스에 올바른 IP 주소 및 서브넷 마스크가 있는지 확인합니다.

디렉터리 서버는 외부 네트워크에 있습니다.

디렉터리 서버가 외부(업링크) 인터페이스의 다른 쪽에 있는 네트워크에 있는 경우, 사이트 대 사이트 VPN 연결을 구성해야 할 수 있습니다. 자세한 절차는 원격 액세스 VPN을 통해 외부 네트워크에서 디렉터리 서버를 사용하는 방법를 참조하십시오.

RADIUS 서버 및 그룹

RADIUS 서버를 사용하여 원격 액세스 VPN 연결과 device manager 및 위협 방어 CLI 관리 사용자를 인증하고 권한을 부여할 수 있습니다. 예를 들어 Cisco ISE(Identity Services Engine) 및 해당 RADIUS 서버도 사용하는 경우에는 이 서버를 device manager에 사용할 수 있습니다.

RADIUS 서버를 사용하도록 기능을 구성할 때는 개별 서버 대신 RADIUS 그룹을 선택합니다. RADIUS 그룹은 서로의 복사본인 RADIUS 서버가 모인 컬렉션입니다. 그룹에 서버가 여러 개 포함된 경우 이러한 서버는 백업 서버 체인을 형성하여 한 서버를 사용할 수 없는 경우 이중화를 제공합니다. 하지만 서버가 하나뿐이더라도 멤버가 하나인 그룹을 생성하여 기능에 대한 RADIUS 지원을 구성해야 합니다.

다음 주제에서는 RADIUS 서버와 그룹을 지원되는 기능에서 사용할 수 있도록 RADIUS 서버와 그룹을 구성하는 방법을 설명합니다.

RADIUS 서버 구성

RADIUS 서버는 AAA(인증, 권한 부여 및 계정 관리) 서비스를 제공합니다. RADIUS 서버를 통해 사용자를 인증하고 권한을 부여하는 경우 device manager에 해당 서버를 사용할 수 있습니다.

각 RADIUS 서버에 해당하는 개체를 생성한 후에는 각 중복 서버 그룹을 포함할 RADIUS 서버 그룹을 생성합니다.

시작하기 전에

RA VPN에 대해 리디렉션 ACL을 컨피그레이션하려는 경우, 서버 개체를 생성 또는 수정하기 전에 스마트 CLI를 사용해 확장된 ACL을 생성해야 합니다. 개체를 수정하는 동안에는 ACL을 생성할 수 없습니다.

프로시저

단계 **1** 목차에서 **Objects(**개체**)**와 **Identity Sources(ID** 소스**)**를 차례로 선택합니다.

단계 **2** 다음 중 하나를 수행합니다.

- 개체를 생성하려면 **+** > **RADIUS Server(RADIUS** 서버**)**를 클릭합니다.
- 개체를 수정하려면 개체의 수정 아이콘( )을 클릭합니다.

참조되지 않는 개체를 삭제하려면 해당 개체의 휴지통 아이콘( )을 클릭합니다.

단계 **3** 다음 속성을 구성합니다.

- **Name(**이름**)** - 개체의 이름입니다. 이 이름은 서버에 구성된 항목과 일치하지 않아도 됩니다.
- **Server Name or IP Address(**서버 이름 또는 **IP** 주소**)** - 서버의 정규화된 호스트 이름(FQDN) 또는 IP 주소입니다. 예를 들어 radius.example.com 또는 10.100.10.10을 입력합니다.

- **Authentication Port(**인증 포트**)** - RADIUS 인증 및 권한 부여가 수행되는 포트입니다. 기본값은 1,812입니다.
- **Timeout(**시간 제한**)** - 시스템이 다음 서버로 요청을 보내기 전까지 서버의 응답을 기다리는 시간(1~300초)입니다. 기본값은 10초입니다. 이 서버를 원격 액세스 VPN에 대한 보조 인증 소스로 사용하는 경우(예: 인증 토큰을 요청하는 메시지 표시), 이 시간제한을 60초 이상으로 높일 수 있습니다. 이를 통해 사용자가 토큰을 획득해 입력할 시간을 제공합니다.
- **Server Secret Key(**서버 비밀 키**)** - (선택 사항). 위협 방어 디바이스와 RADIUS 서버 간의 데이터를 암호화하는 데 사용되는 공유 암호입니다. 이 키는 대/소문자를 구분하며 공백은 포함하지 않는 영숫자 문자열(최대 64자)입니다. 또한 영숫자 문자 또는 밑줄로 시작해야 하며 특수 문자 $ & - _ . + @는 포함할 수 없습니다. 문자열은 RADIUS 서버에 구성된 것과 일치해야 합니다. 비밀 키를 구성하지 않으면 연결이 암호화되지 않습니다.

단계 **4** (선택 사항). 원격 액세스 VPN 권한 부여 변경 컨피그레이션을 위해 서버를 사용 중인 경우, **RA VPN Only(RA VPN**만**)** 링크를 클릭하여 다음 옵션을 컨피그레이션할 수 있습니다.

- **Redirect ACL(**리디렉션 **ACL)** - RA VPN 리디렉션 ACL에 사용할 확장 ACL을 선택합니다. **Device(**장치**)** > **Advanced Configuration(**고급 구성**)** > **Smart CLI(**스마트 **CLI)** > **Objects(**개체**)** 페이지에서 스마트 CLI **Extended Access List(**확장 액세스 목록**)** 개체를 사용하여 확장 ACL을 생성합니다.

  리디렉션 ACL의 목적은 Cisco ISE(Identity Services Engine)에 초기 트래픽을 전송하여 ISE에서 클라이언트 보안 상태를 평가할 수 있게 하는 것입니다. ACL에서는 ISE에 HTTPS 트래픽을 전송해야 하지만, 이미 ISE가 대상으로 지정된 트래픽 또는 이름 확인을 위해 DNS 서버로 전송되는 트래픽은 전송해서는 안 됩니다. 예시는 Threat Defense 디바이스에서 COA(Change of Authorization) 컨피그레이션를 참조하십시오.

- **Interface Used to Connect to RADIUS Server(RADIUS** 서버에 연결하는 데 사용할 인터페이스**)** - 서버와 통신할 때 사용할 인터페이스를 결정합니다. **Resolve via Route Lookup(**경로 조회를 통해 확인**)**을 선택하면 시스템에서는 항상 라우팅 테이블을 사용해 어떤 인터페이스를 사용할지 결정합니다. **Manually Choose Interface(**수동으로 인터페이스 선택**)**를 선택하면 시스템에서는 선택한 인터페이스를 항상 사용합니다.

  CoA(Change of Authorization)를 컨피그레이션하려면 시스템에서 인터페이스의 CoA 리스너를 올바르게 활성화할 수 있도록 특정 인터페이스를 선택해야 합니다.

  서버가 관리 주소와 동일한 네트워크에 있는 경우(진단 인터페이스 선택을 의미함), 진단 인터페이스의 IP 주소도 설정해야 합니다. 관리 IP 주소로는 충분하지 않습니다. **Device(**디바이스**)** > **Interfaces(**인터페이스**)**로 이동하여 관리 IP 주소와 동일한 서브넷에 있는 진단 인터페이스에서 IP 주소를 설정합니다.

  또한 device manager 관리 액세스를 위해 이 서버를 사용하는 경우, 이 인터페이스는 무시됩니다. 관리 액세스 시도는 항상 관리 IP 주소를 통해 인증됩니다.

단계 **5** (선택 사항, 개체 수정 시에만 사용함.) **Test(**테스트**)**를 클릭하여 시스템이 서버에 연결할 수 있는지 확인합니다.

사용자 이름과 비밀번호를 입력하라는 메시지가 표시됩니다. 테스트에서는 서버에 연결할 수 있는지, 그리고 서버에 연결할 수 있는 경우 사용자 이름을 인증할 수 있는지를 확인합니다.

단계 **6** **OK(**확인**)**를 클릭합니다.

RADIUS 서버 그룹 구성

RADIUS 서버 그룹은 하나 이상의 RADIUS 서버 개체를 포함합니다. 그룹 내의 서버는 서로의 복사본이어야 합니다. 이러한 서버는 백업 서버 체인을 형성하므로 첫 번째 서버를 사용할 수 없는 경우 시스템이 목록의 다음 서버 사용을 시도할 수 있습니다.

특정 기능에서 RADIUS 지원을 구성할 때는 서버 그룹을 선택해야 합니다. 따라서 RADIUS 서버가 하나뿐이더라도 해당 서버를 포함하는 서버 그룹을 생성해야 합니다.

프로시저

단계 **1** 목차에서 **Objects(**개체**)**와 **Identity Sources(ID** 소스**)**를 차례로 선택합니다.

단계 **2** 다음 중 하나를 수행합니다.

- 개체를 생성하려면 **+** > **RADIUS Server Group(RADIUS** 서버 그룹**)**을 클릭합니다.
- 개체를 수정하려면 개체의 수정 아이콘( )을 클릭합니다.

참조되지 않는 개체를 삭제하려면 해당 개체의 휴지통 아이콘( )을 클릭합니다.

단계 **3** 다음 속성을 구성합니다.

- **Name(**이름**)** - 개체의 이름입니다. 이 이름은 서버에 구성된 항목과 일치하지 않아도 됩니다.
- **Dead Time(**비활성 시간**)** - 모든 서버에서 장애가 발생해야 장애 발생 서버가 다시 활성화됩니다. 비활성 시간이란 마지막 서버가 실패한 이후, 모든 서버를 재활성화하기 이전의 대기 시간(0~1440분)입니다. 기본은 10분입니다.
- **Maximum Failed Attempts(**최대 실패 시도 횟수**)** - 다음 서버 사용을 시도하기 전에 그룹의 RADIUS 서버로 전송되었으나 실패한 AAA 트랜잭션(즉, 응답을 받지 못한 요청)의 수입니다. 1~5 사이의 값을 지정할 수 있으며 기본값은 3입니다. 최대 실패 시도 횟수가 초과되면 시스템에서 해당 서버를 Failed(장애 발생)로 표시합니다.

  특정 기능에 대해 로컬 데이터베이스를 사용하여 대체 방법을 구성했는데 그룹의 모든 서버가 응답하지 않으면 해당 그룹은 응답이 없는 것으로 간주되고 대체 방법을 시도합니다. 서버 그룹은 데드 타임 동안 응답하지 않는 것으로 표시된 상태를 유지하므로 해당 기간 내의 추가 AAA 요청은 서버 그룹에 연결을 시도하지 않으며 폴백 방법이 즉시 사용됩니다.
- **Dynamic Authorization(**동적 인증**)(RA VPN**에만 해당**)**, **Port(**포트**)** - RADIUS 동적 인증 또는 이 RADIUS 서버 그룹에 대한 CoA(Change of Authorization) 서비스를 활성화할 경우, 해당 그룹은 CoA 알림이 등록되며 ISE(Identity Services Engine)의 CoA 정책 업데이트를 위해 지정된 포트를 수신합니다. 기본 수신 포트는 1700입니다. 또는 1024~65535 범위 내에서 다른 포트를 지정할 수 있습니다. ISE와 함께 원격 액세스 VPN에서 이 서버 그룹을 사용하는 경우에만 동적 인증을 활성화합니다.

- **Realm that Supports the RADIUS Server(RADIUS** 서버를 지원하는 영역**)** - 사용자 인증을 위해 AD 서버를 사용하도록 RADIUS 서버를 컨피그레이션하는 경우, 이 RADIUS 서버와 함께 사용되는 AD 서버를 지정하는 AD 영역을 선택합니다. 영역이 아직 없는 경우, 목록 아래에 있는 **Create New Identity Realm(**새 **ID** 영역 생성**)**을 클릭하여 영역을 바로 컨피그레이션합니다.
- **RADIUS Server list(RADIUS** 서버 목록**)** - 그룹의 서버를 정의하는 RADIUS 서버 개체를 16개까지 선택합니다. 이러한 개체는 우선순위대로 추가합니다. 목록의 첫 번째 서버가 응답이 없는 상태가 될 때까지 계속 사용됩니다. 개체를 추가한 후에는 끌어 놓기를 통해 개체를 다시 정렬할 수 있습니다. 필요한 개체가 아직 없으면 **Create New RADIUS Server(**새 **RADIUS** 서버 생성**)**를 클릭하여 바로 추가합니다.

  Test(테스트**)** 링크를 클릭하여 시스템이 서버에 연결할 수 있는지를 확인할 수도 있습니다. 사용자 이름과 비밀번호를 입력하라는 메시지가 표시됩니다. 테스트에서는 서버에 연결할 수 있는지, 그리고 서버에 연결할 수 있는 경우 사용자 이름을 인증할 수 있는지를 확인합니다.

단계 **4** (선택 사항). **Test All Servers(**모든 서버 테스트**)** 버튼을 클릭하여 그룹의 각 서버에 대한 연결을 확인합니다.

사용자 이름과 비밀번호를 입력하라는 메시지가 표시됩니다. 시스템은 각 서버에 연결할 수 있는지, 그리고 각 서버에서 사용자 이름을 인증할 수 있는지를 확인합니다.

단계 **5** **OK(**확인**)**를 클릭합니다.

RADIUS 서버 및 그룹 트러블슈팅

외부 권한 부여가 작동하지 않는 경우 확인할 수 있는 몇 가지 사항은 다음과 같습니다.

- RADIUS 서버 및 서버 그룹 개체의 **Test(**테스트**)** 버튼을 사용하여 디바이스에서 서버에 연결할 수 있는지 확인합니다. 테스트 전에 개체를 저장해야 합니다. 테스트에 실패하는 경우 다음을 수행합니다.
  - 테스트에서 서버에 대해 구성된 인터페이스를 무시하고 항상 관리 인터페이스를 사용한다는 점을 이해하십시오. RADIUS 인증 프록시가 관리 IP 주소의 요청에 응답하도록 구성되지 않은 경우 테스트는 실패할 것으로 예상됩니다.
  - 테스트 중에 정확한 사용자 이름/비밀번호 조합을 입력했는지 확인합니다. 이러한 정보가 부정확한 경우에는 Bad Credentials(잘못된 크리덴셜) 메시지가 표시됩니다.
  - 서버의 비밀 키, 포트 및 IP 주소를 확인합니다. 호스트 이름을 사용하는 경우 관리 인터페이스에 대해 DNS가 구성되어 있는지 확인합니다. 비밀 키가 RADIUS 서버에서는 변경되었는데 디바이스 컨피그레이션에서는 변경되지 않았을 가능성을 고려합니다.
  - 테스트에 계속 실패하면 RADIUS 서버에 대한 정적 경로를 구성해야 할 수 있습니다. CLI 콘솔이나 SSH 세션에서 서버에 ping을 시도하여 서버에 연결할 수 있는지 확인합니다.
- 이전에는 작동한 외부 인증이 중지된 경우 모든 서버가 비활성 시간에 있는 가능성을 고려합니다. 특정 그룹 내의 모든 RADIUS 서버에 장애가 발생한 경우 비활성 시간은 첫 번째 서버 연결

을 다시 시도할 때까지 시스템이 대기하는 시간(분)입니다. 기본값은 10분이지만 최대 1440분까지 구성할 수 있습니다.

- HTTPS 외부 인증이 일부 사용자에 대해서만 작동하는 경우, 각 사용자 계정에 대해 RADIUS 서버에 정의된 cisco-av-pair 속성을 평가합니다. 이 특성이 올바르지 않게 구성되어 있을 수 있습니다. 속성이 누락되거나 올바르지 않은 경우, 해당 사용자 계정에 대한 모든 HTTS 액세스가 차단됩니다.
- SSH 외부 인증이 일부 사용자에 대해서만 작동하는 경우, 각 사용자 계정에 대해 RADIUS 서버에 정의된 Service-Type 속성을 평가합니다. 이 특성이 올바르지 않게 구성되어 있을 수 있습니다. 속성이 누락되거나 올바르지 않은 경우, 해당 사용자 계정에 대한 모든 SSH 액세스가 차단됩니다.

Identity Services Engine (ISE)

Cisco ISE(Identity Services Engine) 또는 ISE-PIC(ISE Passive Identity Connector) 구축을 위협 방어 디바이스와 통합하여 ISE/ISE-PIC를 패시브 인증에 사용할 수 있습니다.

신뢰할 수 있는 ID 소스인 ISE/ISE-PIC는 AD(Active Directory), LDAP, RADIUS 또는 RSA를 사용하여 인증하는 사용자에 대한 사용자 인식 데이터를 제공합니다. 그러나 위협 방어의 경우에는 사용자 ID 인식을 위해 ISE를 사용할 때 AD만 사용할 수 있습니다. 사용자 ID를 액세스 제어 및 SSL 암호 해독 정책에서 일치 기준으로 사용할 수 있습니다. 또한 다양한 모니터링 대시보드 및 이벤트에서 사용자 정보를 확인할 수 있습니다.

Cisco ISE/ISE-PIC에 대한 자세한 내용은 *Cisco Identity Services Engine* 관리자 가이드 (https://www.cisco.com/c/en/us/support/security/identity-services-engine/tsd-products-support-series-home.html) 및 *ISE-PIC(Identity Services Engine Passive Identity Connector)* 설치 및 관리자 가이드(https://www.cisco.com/c/en/us/support/security/ise-passive-identity-connector/tsd-products-support-series-home.html)를 참조하십시오.

ISE에 대한 지침 및 제한 사항

- 방화벽 시스템에서는 Active Directory 인증과 함께 802.1x 디바이스 인증을 지원하지 않습니다. 이는 시스템에서 디바이스 인증을 사용자에게 연결하지 않기 때문입니다. 802.1x 활성 로그인을 사용하는 경우에는 802.1x 활성 로그인(디바이스와 사용자 둘 다)만 보고하도록 ISE를 구성합니다. 이렇게 하면 디바이스 로그인이 시스템에 한 번만 보고됩니다.
- ISE/ISE-PIC에서는 ISE 게스트 서비스 사용자의 활동을 보고하지 않습니다.
- ISE/ISE-PIC 서버와 디바이스의 시간을 동기화합니다. 그렇지 않으면 시스템이 예기치 않은 간격으로 사용자 시간 제한을 수행할 수 있습니다.
- 많은 사용자 그룹을 모니터링하도록 ISE-PIC를 구성하는 경우 시스템은 메모리 제한으로 인해 그룹을 기준으로 사용자 매핑을 삭제할 수 있습니다. 그 결과, 영역이 있는 규칙 또는 사용자 조건이 정상적으로 수행되지 않을 수 있습니다.

- 이 시스템 버전과 호환되는 특정 ISE/ISE-PIC 버전에 대한 자세한 내용은 *Cisco Secure Firepower* 호환성 가이드https://www.cisco.com/c/en/us/support/security/firepower-ngfw/products-device-support-tables-list.html를 참고하십시오.
- 사용 중인 ISE 버전이 IPv6을 지원하는지 확인하지 않았다면 ISE 서버의 IPv4 주소를 사용하십시오.

ISE(Identity Services Engine) 구성

Cisco ISE(Identity Services Engine) 또는 Cisco ISE PIC(Identity Services Engine Passive Identity Connector)를 패시브 ID 소스로 사용하려면 ISE pxGrid(Platform Exchange Grid) 서버에 대한 연결을 구성해야 합니다.

시작하기 전에

- ISE에서 pxGrid 및 MNT 서버 인증서를 내보냅니다. 예를 들어 ISE PIC 2.2에서는 **Certificates(**인증서**)** > **Certificate Management(**인증서 관리**)** > **System Certificates(**시스템 인증서**)** 페이지에서 이러한 인증서를 확인할 수 있습니다. 인증서 목록의 Used By(사용한 사람) 열에는 MNT(모니터링 및 트러블슈팅 노드)가 Admin(관리자)로 표시됩니다. 인증서는 **Objects(**개체**)** > **Certificates(**인증서**)** 페이지에서 신뢰할 수 있는 CA 인증서로 업로드할 수도 있고 다음 절차 중에 업로드할 수도 있습니다. 이러한 노드는 동일한 인증서를 사용 중일 수 있습니다.
- AD ID 영역도 구성해야 합니다. 시스템은 AD에서 사용자 목록을 가져오며 ISE에서 사용자-IP 주소 매핑 정보를 가져옵니다.
- 정적 보안 그룹 태그 매핑을 사용하거나 사용하지 않고 액세스 제어에 SGT(Security Group Tag)를 사용하여 SXP 주제를 수신하려면 ISE에 SXP 및 이러한 매핑을 구성해야 합니다. ISE에서 보안 그룹 및 SXP 게시 구성의 내용을 참조하십시오.

프로시저

단계 **1** 목차에서 **Objects(**개체**)**와 **Identity Sources(ID** 소스**)**를 차례로 선택합니다.

단계 **2** 다음 중 하나를 수행합니다.

- 개체를 생성하려면 **+** > **ISE(Identity Services Engine)**를 클릭합니다. ISE 개체는 하나까지만 생성할 수 있습니다.
- 개체를 수정하려면 개체의 수정 아이콘()을 클릭합니다.

참조되지 않는 개체를 삭제하려면 해당 개체의 휴지통 아이콘()을 클릭합니다.

단계 **3** 다음 속성을 구성합니다.

- **Name(**이름**)** - 개체의 이름입니다.
- **Status(**상태**)** - 토글을 클릭하여 개체를 활성화하거나 비활성화합니다. 비활성화하면 ID 규칙에서 ISE를 ID 소스로 사용할 수 없습니다.

- **Description(**설명**)** - 개체의 설명(선택 사항)입니다.
- **Primary Node Hostname/IP Address(**기본 노드 호스트 이름**/IP** 주소**)** - 기본 pxGrid ISE 서버의 호스트 이름 또는 IP 주소입니다. 사용 중인 ISE 버전이 IPv6을 지원하는지 확인하지 않았다면 IPv6 주소를 지정하지 마십시오.
- **Secondary Node Hostname/IP Address(**보조 노드 호스트네임**/IP** 주소**)** - 고가용성을 위해 보조 ISE 서버를 설정하는 경우, **Add Secondary Node Hostname/IP Address(**보조 노드 호스트네임**/IP** 주소 추가**)**를 클릭하고 보조 pxGrid ISE 서버의 호스트네임 또는 IP 주소를 입력합니다.
- **pxGrid Server CA Certificate(pxGrid** 서버 **CA** 인증서**)** - 신뢰할 수 있는 pxGrid 프레임워크용 인증 기관 인증서입니다. 구축에 기본 및 보조 pxGrid 노드가 포함된 경우 동일한 인증 증명으로 두 가지 노드의 인증서를 서명해야 합니다.
- **MNT Server CA Certificate(MNT** 서버 **CA** 인증서**)** - 일괄 다운로드를 수행할 때 신뢰할 수 있는 ISE 인증서용 인증 기관 인증서입니다. MNT(모니터링 및 트러블슈팅) 서버가 별도로 지정되어 있지 않은 경우 pxGrid 서버 인증서와 같을 수 있습니다. 구축에 기본 및 보조 MNT 노드가 포함된 경우 동일한 인증 증명으로 두 가지 노드의 인증서를 서명해야 합니다.
- **Server Certificate(**서버 인증서**)** - ISE에 연결하거나 일괄 다운로드를 수행할 때 위협 방어 디바이스가 ISE에 제공해야 하는 내부 ID 인증서입니다.
- **Subscribe To(**구독 대상**)** — 어떤 ISE pxGrid 주제를 구독할지 선택합니다. 주제를 구독하면 해당 주제와 관련된 데이터를 다운로드할 수 있습니다.
  - **Session Directory Topic(**세션 디렉토리 주제**)** — 사용자 세션에 대한 SGT 매핑을 비롯한 사용자 세션에 대한 정보를 가져올지 여부입니다. 이 옵션은 기본적으로 활성화되어 있습니다. 보안 정책에 사용하고 모니터링 대시보드에서 볼 수 있도록 패시브 사용자 ID를 가져오려면 이 옵션을 선택해야 합니다.
  - **SXP Topic(SXP** 주제**)** — 정적 SGT-IP 주소 매핑을 가져올지 여부입니다. SGT(Security Group Tag)를 기반으로 액세스 제어 규칙을 작성하려면 이 항목을 선택합니다.
- **ISE Network Filters(ISE** 네트워크 필터**) - ISE**가 시스템에 보고하는 데이터를 제한하기 위해 설정할 수 있는 선택적 필터입니다. 네트워크 필터를 제공하는 경우 ISE는 필터 내의 네트워크에서만 데이터를 보고합니다. **+**를 클릭하고 네트워크를 식별하는 네트워크 개체를 선택한 후에 **OK(**확인**)**를 클릭합니다. 개체를 생성해야 하는 경우 **Create New Network(**새 네트워크 생성**)**를 클릭합니다. IPv4 네트워크 개체만 구성합니다.

단계 **4** **Test(**테스트**)** 버튼을 클릭하여 시스템이 ISE 서버에 연결할 수 있는지 확인합니다.

테스트에 실패하는 경우 **See Logs(**로그 보기**)** 링크를 클릭하여 자세한 오류 메시지를 확인합니다. 예를 들어 다음 메시지는 시스템이 필요한 포트에서 서버에 연결하지 못했음을 나타냅니다. 호스트로의 경로가 없거나, ISE 서버가 필요한 포트를 사용하고 있지 않거나, 연결을 차단하는 액세스 제어 규칙이 문제일 수 있습니다.

```
Captured Jabberwerx log:2018-05-11T16:10:30 [   ERROR]: connection timed out while
trying to test connection to host=10.88.127.142:ip=10.88.127.142:port=5222
```

단계 **5** **OK(**확인**)**를 클릭하여 개체를 저장합니다.

다음에 수행할 작업

ISE를 구성한 후 ID 정책을 활성화하고, 패시브 인증 규칙을 구성하고, 컨피그레이션을 구축합니다. 그런 다음 ISE/ISE PIC로 이동하여 디바이스를 서브스크라이버로 수락해야 합니다. ISE/ISE PIC가 서브스크라이버를 자동 수락하도록 구성하면 서브스크립션을 수동으로 수락할 필요가 없습니다.

ISE/ISE-PIC ID 소스 트러블슈팅

ISE/ISE-PIC 연결

ISE 또는 ISE-PIC 연결에 문제가 발생한 경우 다음을 확인하십시오.

- ISE를 위협 방어 디바이스와 성공적으로 통합하려면 우선 ISE에서 pxGrid Identity Mapping(pxGrid ID 매핑) 기능을 활성화해야 합니다.
- ISE 서버와 위협 방어 디바이스 간의 연결에 성공하려면 ISE에서 클라이언트를 수동으로 승인해야 합니다.

  Cisco Identity Services Engine 관리자 가이드의 사용자 및 외부 ID 소스 관리 장에서 설명하는 것처럼 ISE에서 **Automatically approve new accounts(**새 어카운트 자동 승인**)**를 활성화할 수도 있습니다.
- 위협 방어 디바이스(서버) 인증서는 **clientAuth** 확장 키 사용 값을 포함해야 하거나 아무 확장 키 사용 값도 포함하지 않아야 합니다. clientAuth 확장 키 사용이 설정되어 있는 경우에는 키 사용이 설정되어 있지 않거나 디지털 서명 키 사용 값이 설정되어 있어야 합니다. device manager를 사용하여 생성할 수 있는 자체 서명 ID 인증서는 이러한 요구 사항을 충족합니다.
- ISE 서버의 시간은 위협 방어 디바이스의 시간과 동기화되어야 합니다. 어플라이언스가 동기화되지 않은 경우, 시스템이 예기치 않은 간격으로 사용자 시간 제한을 수행할 수 있습니다.

ISE/ISE-PIC 사용자 데이터

ISE 또는 ISE-PIC에서 보고된 사용자 데이터에 문제가 발생한 경우 다음을 참고하십시오.

- 데이터베이스에 데이터가 아직 없는 ISE 사용자의 활동이 탐지되면 시스템은 서버에서 관련된 정보를 검색합니다. 시스템이 사용자 다운로드에서 사용자에 대한 정보를 성공적으로 검색할 때까지는 ISE 사용자가 확인한 활동이 액세스 제어 규칙으로 처리되지 않으며, 대시보드에 표시되지도 않습니다.
- LDAP, RADIUS 또는 RSA 도메인 컨트롤러에서 인증된 ISE 사용자에 대해서는 사용자 제어를 수행할 수 없습니다.
- 시스템은 ISE 게스트 서비스 사용자의 사용자 데이터를 수신하지 않습니다.

SAML 서버

원격 액세스 VPN 연결를 위한 SSO(Single Sign-On) 인증 소스로 사용할 SAML 2.0(Security Assertion Markup Language 2.0) 서버를 구성할 수 있습니다. SAML은 당사자 간에 인증 및 권한 부여 데이터, 특히 IdP(Identity Provider)와 SP(Service Provider)를 교환하기 위한 개방형 표준입니다.

참고 지원되는 SAML 서버: Duo

SAML 서버 구성

원격 액세스 VPN 연결를 위한 SSO(Single Sign-On) 인증 소스로 사용할 SAML 2.0(Security Assertion Markup Language 2.0) 서버를 구성할 수 있습니다. 예를 들어 DAG(Duo Access Gateway)는 SAML 서버입니다.

SAML 서버를 인증 방법으로 사용하는 경우 SAML 서버는 IdP(Identity Provider)로 작동하는 반면 threat defense 디바이스는 SP(Service Provider)로 작동합니다.

RA VPN의 경우 SAML 서버를 기본 인증 소스로 사용할 수 있지만 보조 인증 소스를 구성할 수 없으며 대체 소스를 구성할 수도 없습니다.

시작하기 전에

SAML 서버 ID 공급자에서 다음 정보를 가져옵니다.

- SAML 서버 메타데이터를 제공하는 엔티티 ID URL
- 로그인 URL
- 로그아웃 URL
- ID 공급자 인증서

프로시저

단계 **1** 다음 중 하나를 수행하여 SAML 서버 페이지로 이동합니다.

- 목차에서 **Objects(**개체**)**와 **Identity Sources(ID** 소스**)**를 차례로 선택합니다.
- **Device(**디바이스**)** > **Remote Access VPN(**원격 액세스 **VPN)** > **SAML Servers(SAML** 서버**)**를 선택합니다.

단계 **2** 다음 중 하나를 수행합니다.

- 개체를 생성하려면 **+** > **SAML Server(SAML** 서버**)**를 클릭합니다.
- 개체를 수정하려면 개체의 수정 아이콘( )을 클릭합니다.

참조되지 않는 개체를 삭제하려면 해당 개체의 휴지통 아이콘( )을 클릭합니다.

단계 **3** 다음 속성을 구성합니다.

- **Name(**이름**)** - 개체의 이름입니다.
- **Description(**설명**)** - 개체의 설명(선택 사항)입니다.
- **Identity Provider (IDP) Entity ID URL(IdP(ID** 공급자**)** 엔티티 **ID URL)** — SAML 발급자가 요청에 응답하는 방법을 설명하는 메타데이터 XML을 제공하는 페이지의 URL입니다. 일부 SAML 서버 제품에서는 이를 엔티티 ID라고 하고, 일부는 메타데이터 URL이라고 합니다. URL은 프로토콜 https://를 포함하여 4~256자 사이여야 합니다. (예: https://191.168.2.21/dag/saml2/idp/metadata.php)
- **Sign-In URL(**로그인 **URL)** — ID 공급자 SAML 서버에 로그인하기 위한 URL입니다. URL은 프로토콜을 포함하여 4~500자 사이여야 합니다. http:// 및 https:// 모두 허용됩니다. (예: https://191.168.2.21/dag/saml2/idp/SSOService.php)
- **Sign-Out URL(**로그아웃 **URL)** - ID 공급자 SAML 서버에서 로그아웃하기 위한 URL입니다. URL은 프로토콜을 포함하여 4~500자 사이여야 합니다. http:// 및 https:// 모두 허용됩니다. (예: https://191.168.2.21/dag/saml2/idp/SingleLogoutService.php)
- **Service Provider Certificate(FTD** 서비스 공급자 인증서**)** — threat defense 디바이스에 사용할 내부 인증서입니다. 원칙적으로는 인증된 서드 파티에서 서명한 인증서를 이미 업로드했으므로 지금 선택할 수 있습니다. 또한 내장된 DefaultInternalCertificate를 사용하거나 **Create New Internal Certificate(**새 내부 인증서 생성**)**를 클릭하여 서명된 인증서를 지금 업로드할 수도 있습니다. SAML 서버 ID 공급자는 이 인증서를 신뢰해야 하므로 SAML 서버에 이를 업로드해야 할 수 있습니다. 인증서를 업로드하거나 서비스 공급자와의 신뢰 관계를 활성화하는 방법에 대한 자세한 내용은 SAML 서버 설명서를 참조하십시오.
- **Identity Provider Certificate(ID** 공급자 인증서**)** — SAML 서버 ID 공급자에 대해 신뢰할 수 있는 CA 인증서입니다. SAML 서버에서 이 인증서를 다운로드합니다. 아직 업로드하지 않은 경우 **Create New Trusted CA Certificate(**새 신뢰할 수 있는 **CA** 인증서 생성**)**를 클릭하여 지금 업로드합니다.
- **Request Signature(**서명 요청**)** — 로그인 요청에 서명할 때 사용할 암호화 알고리즘입니다. 암호화를 비활성화하려면 None(없음)을 선택합니다. 그렇지 않은 경우에는 SHA1, SHA256, SHA384, SHA512(가장 약한 순서에서 가장 강한 순서로 나열) 중 하나를 선택합니다.
- **Request Timeout(**요청 시간 초과**)** - SAML 어설션에는 유효 기간이 있습니다. 사용자는 유효 기간 내에 SSO(Single Sign-On) 요청을 완료해야 합니다. 시간 초과(초 단위)를 설정하여 이 기간을 변경할 수 있습니다. 어설션의 NotOnOrAfter 조건보다 긴 값으로 시간 초과를 설정할 경우 이 시간 초과를 무시하고 NotOnOrAfter가 적용됩니다. 범위는 1~7200초입니다. 기본값은 300초입니다.
- **This SAML identity provider (IDP) is on an internal network(**이 **SAML ID** 공급자**(IDP)**가 내부 네트워크에 있습니다**)** — SAML 서버가 보호받는 네트워크의 외부가 아닌 내부 네트워크에서 작동하는지 여부.

- **Request IDP re-authentication at login(**로그인 시 **IDP** 재인증 요청**)** — SAML 서버가 이전 인증 세션을 다시 사용하지 않고 사용자가 로그인할 때마다 재인증하려면 이 옵션을 선택합니다. 이 옵션은 기본적으로 활성화되어 있습니다.

단계 **4** **OK(**확인**)**를 클릭합니다.

로컬 사용자

로컬 사용자 데이터베이스(LocalIdentitySource)에는 device manager에 정의한 사용자가 포함되어 있습니다.

로컬에서 정의된 사용자는 다음과 같은 목적으로 사용할 수 있습니다.

- 원격 액세스 VPN(기본 또는 대체 ID 소스로 사용)
- 관리 액세스(device manager 사용자에 대한 기본 또는 보조 소스로 사용).

  관리 사용자는 시스템 정의 로컬 사용자입니다. 그러나 관리 사용자는 원격 액세스 VPN에 로그인할 수 없습니다. 추가 로컬 관리 사용자를 생성할 수도 없습니다.

  관리 액세스용 외부 인증을 정의하는 경우에는 디바이스에 로그인하는 외부 사용자가 로컬 사용자 목록에 표시됩니다.
- ID 정책(원격 액세스 VPN 로그인에서 사용자 ID를 수집하기 위한 패시브 ID 소스로 간접 사용).

다음 주제에서는 로컬 사용자를 구성하는 방법을 설명합니다.

로컬 사용자 구성

원격 액세스 VPN에 사용할 디바이스에서 직접 사용자 어카운트를 생성할 수 있습니다. 외부 인증 소스 대신 또는 외부 인증 소스와 함께 로컬 사용자 어카운트를 사용할 수 있습니다.

로컬 사용자 데이터베이스를 원격 액세스 VPN용 대체 인증 방법으로 사용하는 경우, 외부 데이터베이스의 이름과 같은 사용자 이름/비밀번호를 로컬 데이터베이스에서 구성해야 합니다. 그렇지 않으면 대체 메커니즘이 적용되지 않습니다.

여기서 정의하는 사용자는 디바이스 CLI에 로그인할 수 없습니다.

프로시저

단계 **1** **Objects(**개체**)** > **Users(**사용자**)**를 선택합니다.

목록에 사용자 이름과 서비스 유형이 표시되며, 다음과 같습니다.

- MGMT - device manager에 로그인할 수 있는 관리 사용자입니다. 관리 사용자는 항상 정의되어 있으며 삭제할 수 없습니다. 추가 MGMT 사용자를 구성할 수도 없습니다. 그러나 관리 액세스용

외부 인증을 정의하는 경우에는 디바이스에 로그인하는 외부 사용자가 로컬 사용자 목록에 MGMT 사용자로 표시됩니다.

- RA VPN - 디바이스에 구성된 원격 액세스 VPN에 로그인할 수 있는 사용자입니다. 기본 또는 보조(대체) 소스용 로컬 데이터베이스도 선택해야 합니다.

단계 **2** 다음 중 하나를 수행합니다.

- 사용자를 추가하려면 +를 클릭합니다.
- 사용자를 수정하려면 해당 사용자의 수정 아이콘()을 클릭합니다.

특정 사용자 어카운트가 더 이상 필요하지 않으면 해당 사용자의 삭제 아이콘()을 클릭합니다.

단계 **3** 사용자 속성을 구성합니다.

이름과 비밀번호는 인쇄 가능한 모든 ASCII 영숫자 또는 특수 문자(공백과 물음표 제외)를 포함할 수 있습니다. 인쇄 가능한 문자는 ASCII 코드 33~126입니다.

- **Name(**이름**)** - 원격 액세스 VPN에 로그인하기 위한 사용자 이름입니다. 이 이름은 4~64자로 지정할 수 있으며 공백은 포함할 수 없습니다. 예를 들어 johndoe와 같은 이름을 사용합니다.
- **Password(**비밀번호**)**, **Confirm Password(**비밀번호 확인**)** - 어카운트의 비밀번호를 입력합니다. 비밀번호는 8~16자여야 하며 같은 문자를 연속으로 포함할 수는 없습니다. 또한 숫자, 대/소문자, 특수 문자를 각각 하나 이상 포함해야 합니다.

참고 사용자는 비밀번호를 변경할 수 없습니다. 관리자가 사용자에게 비밀번호를 알려 주어야 하며, 비밀번호를 변경해야 하는 경우 관리자가 사용자 어카운트를 수정해야 합니다. 또한 외부 MGMT 사용자의 비밀번호는 업데이트하지 마십시오. 해당 비밀번호는 외부 AAA 서버를 통해 제어됩니다.

단계 **4** **OK(**확인**)**를 클릭합니다.