영역

다음 주제에서는 영역 및 ID 정책에 대해 설명합니다.

- 영역 및 영역 시퀀스 정보, 1 페이지
- 영역 라이선스 요건, 9 페이지
- 영역 요구 사항 및 사전 요건, 9 페이지
- Microsoft Azure AD 영역 생성, 10 페이지
- LDAP 영역 또는 Active Directory 영역 및 영역 디렉터리 생성, 19 페이지
- 영역 시퀀스 생성, 34 페이지
- 도메인 간 신뢰를 위한 Management Center 구성: 설정, 35 페이지
- 영역 관리, 43 페이지
- 영역 비교, 44 페이지
- 영역 및 사용자 다운로드 문제 해결, 44 페이지
- 영역 히스토리, 53 페이지

영역 및 영역 시퀀스 정보

영역은 Secure Firewall Management Center와 사용자가 모니터링하는 서버의 사용자 계정 간 연결을 의미합니다. 또한 서버의 연결 설정 및 인증 필터 설정을 지정합니다. 영역에는 다음과 같은 기능이 있습니다.

- 활동을 모니터링할 사용자 및 사용자 그룹을 지정할 수 있습니다.
- 신뢰할 수 있는 사용자는 물론 일부 신뢰할 수 없는 사용자, 즉 트래픽 기반 탐지로 탐지한 POP3 및 IMAP 사용자와 트래픽 기반 탐지로 탐지한 사용자, TS 에이전트 또는 ISE/ISE-PIC의 사용자 메타데이터에 대한 사용자 저장소를 쿼리합니다.

(Microsoft AD 영역만 해당*)* 영역 시퀀스는 ID 정책에 사용할 두 개 이상의 Active Directory 영역으로 구성된 순서가 지정된 목록입니다. 영역 시퀀스를 ID 규칙과 연결할 경우 시스템은 영역 시퀀스에 지정된 순서대로 Active Directory 도메인을 검색합니다.

한 영역 내에 여러 도메인 컨트롤러를 디렉터리로 추가할 수 있지만, 이러한 컨트롤러는 같은 기본 영역 정보를 공유해야 합니다. 영역 내의 디렉터리는 모두 LDAP 서버이거나 모두 AD(Active Directory)

서버여야 합니다. 영역을 활성화하고 나면 다음번에 management center이 서버를 쿼리할 때 저장한 변경 사항이 적용됩니다.

사용자 인식을 수행하려면 영역에 지원되는 서버에 대해 영역을 구성해야 합니다. 시스템은 이러한 연결을 이용해 POP3 및 IMAP 사용자에 연결된 데이터의 서버를 쿼리하고, 트래픽 기반 탐지를 통해 검색한 LDAP 사용자 관련 데이터를 수집합니다.

시스템은 POP3 및 IMAP 로그인에서 이메일 주소를 사용하여 Active Directory, Microsoft Azure Active Directory, 또는 OpenLDAP의 LDAP 사용자에 대해 상관관계를 지정합니다. 예를 들어 매니지드 디바이스가 LDAP 사용자와 동일한 이메일 주소의 사용자에 대해 POP3 로그인을 탐지하면, 시스템은 LDAP 사용자의 메타데이터를 해당 사용자와 연결합니다.

사용자 제어를 수행하려는 경우 다음을 구성할 수 있습니다.

- Active Directory, Microsoft Azure Active Directory, 서버 또는 ISE/ISE-PIC에 대한 영역 또는 영역 시퀀스

참고 사용자, 그룹, 영역, 엔드포인트 위치 또는 엔드포인트 프로파일 조건이 아닌 SGT ISE 속성 조건을 설정하려는 경우 또는 ID 정책을 사용하여 네트워크 트래픽을 필터링하는 경우에만 Microsoft AD 영역 또는 영역 시퀀스 구성이 선택 사항입니다.

Microsoft Azure AD 영역에는 영역 시퀀스를 사용할 수 없습니다.

- TS 에이전트에 대한 Microsoft AD 서버의 영역 또는 영역 시퀀스.
- 캡티브 포털의 경우, LDAP 영역입니다.

  영역 시퀀스는 LDAP에 대해 지원되지 않습니다.

Microsoft AD 그룹을 중첩할 수 있으며, Secure Firewall Management Center에서는 해당 그룹과 포함된 사용자를 다운로드합니다. LDAP 영역 또는 Active Directory 영역 및 영역 디렉터리 생성, 19 페이지에 설명된 대로 다운로드할 그룹 및 사용자를 필요에 따라 제한할 수 있습니다.

사용자 동기화 정보

management center과 LDAP 또는 Microsoft AD 서버 간 연결을 구성하는 영역 또는 영역 시퀀스를 설정해 탐지한 특정 사용자에 대한 사용자 및 사용자 그룹 메타데이터를 검색할 수 있습니다.

- ISE/ISE-PIC에서 보고하거나 캡티브 포털을 통해 인증하는 LDAP 및 Microsoft AD 사용자. 이 메타데이터는 사용자 인식 및 사용자 제어에 사용할 수 있습니다.
- 트래픽 기반 탐지에서 탐지된 POP3 및 IMAP 사용자 로그인(해당 사용자의 이메일 주소가 LDAP 또는 AD 사용자와 동일한 경우). 이 메타데이터는 사용자 인식에 사용할 수 있습니다.

management center에서는 각 사용자에 대한 다음과 같은 정보 및 메타데이터를 얻습니다.

- LDAP 사용자 이름
- 이름 및 성

- 이메일 주소
- 부서
- 전화 번호

중요 Secure Firewall Management Center와 Active Directory 도메인 컨트롤러 간의 레이턴시를 줄이려면 Secure Firewall Management Center와 최대한 지리적으로 가까운 영역 디렉터리(즉, 도메인 컨트롤러)를 구성하는 것이 좋습니다.

예를 들어 Secure Firewall Management Center가 북미에 있는 경우 북미에도 있는 영역 디렉터리를 구성합니다. 그렇지 않으면 사용자 및 그룹 다운로드 시간 초과 등의 문제가 발생할 수 있습니다.

사용자 활동 데이터 정보

사용자 활동 데이터는 사용자 활동 데이터베이스에 저장되며 사용자 ID 데이터는 사용자 데이터베이스에 저장됩니다. 액세스 컨트롤에서 저장하고 사용할 수 있는 최대 사용자 수는 management center 모델에 따라 달라집니다. 포함할 사용자 및 그룹을 선택할 때는 총 사용자 수가 모델 제한보다 작은지 확인하십시오. 액세스 컨트롤 파라미터가 너무 광범위하면, management center에서는 최대한 많은 사용자의 정보를 가져오며 검색에 실패한 사용자 수를 메시지 센터의 Tasks(작업) 탭 페이지에 보고합니다.

선택적으로 매니지드 디바이스가 사용자 인식 데이터를 감시하는 서브넷을 제한하기 위해 Cisco Secure Firewall Threat Defense 명령 참조에 설명된 대로 **configure identity-subnet-filter** 명령을 사용할 수 있습니다.

참고 사용자 저장소에서 시스템이 탐지한 사용자를 제거할 경우, management center은(는) 절대로 사용자 데이터베이스에서 해당 사용자를 제거하지 않습니다. 반드시 수동으로 삭제해야 합니다. 그러나 management center이(가) 신뢰할 수 있는 사용자 목록을 다음에 업데이트할 때 LDAP 변경 사항이 액세스 컨트롤 규칙에 반영됩니다.

영역 및 신뢰할 수 있는 도메인

management center에서 Microsoft Active Directory (AD) 영역을 구성하면 Microsoft Active Directory 또는 LDAP 도메인과 연결됩니다.

서로를 신뢰하는 Microsoft Active Directory (AD) 도메인은 일반적으로 *forest(*포레스트*)*라고 합니다. 이 신뢰 관계는 도메인이 다양한 방법으로 서로의 리소스에 액세스하게 할 수 있습니다. 예를 들어 도메인 A에 정의된 사용자 계정은 도메인 B에 정의된 그룹의 멤버로 표시할 수 있습니다.

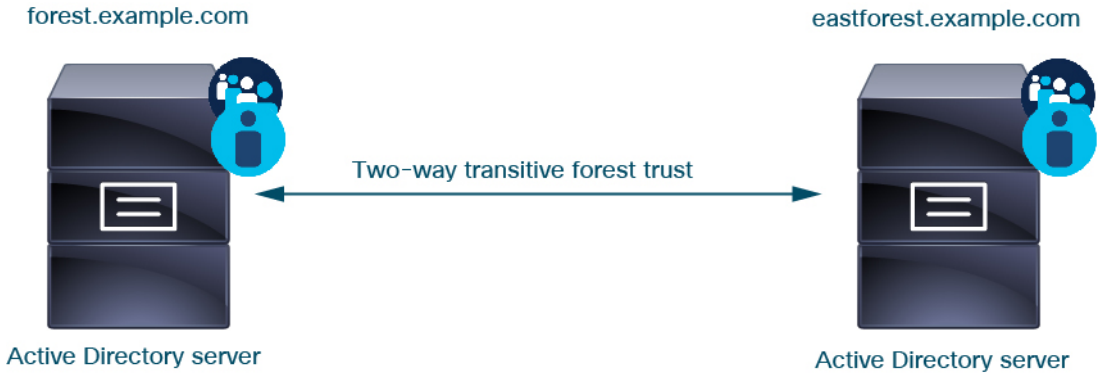
참고 신뢰할 수 있는 도메인은 Microsoft Active Directory 도메인에만 적용됩니다. Microsoft Azure Active Directory 또는 LDAP 도메인에는 적용되지 않습니다.

시스템 및 신뢰할 수 있는 도메인

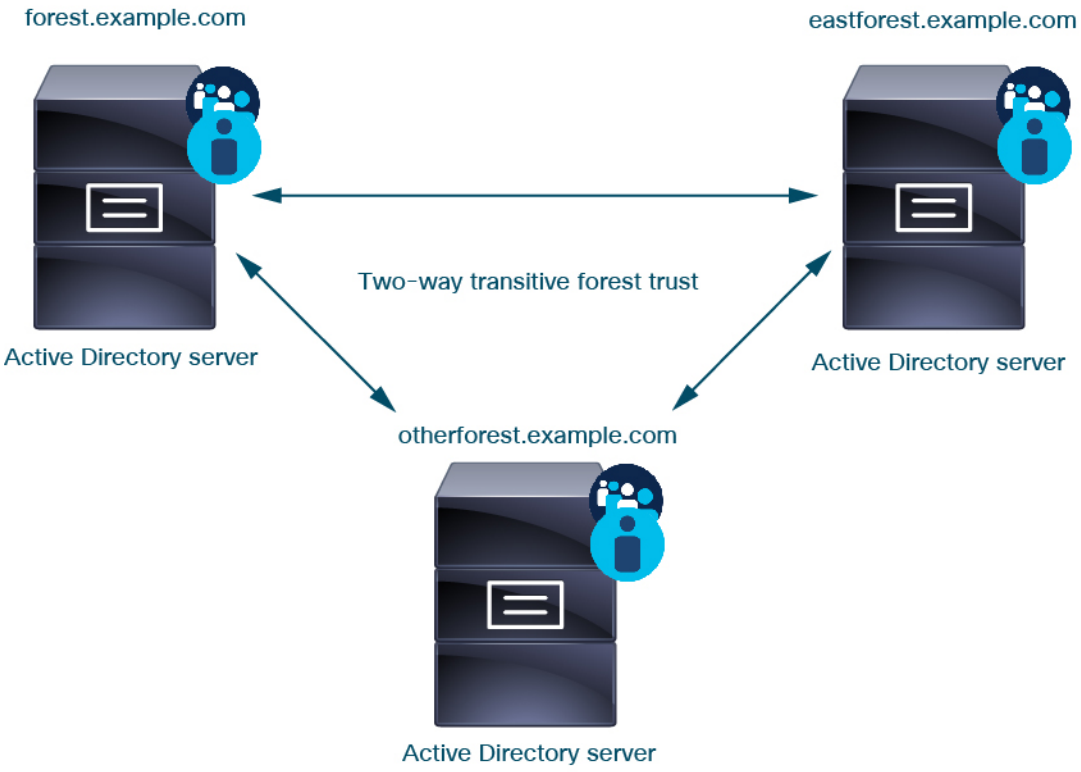
시스템은 신뢰 관계에서 설정된 AD 포리스트를 지원합니다. 신뢰 관계에는 여러 가지 유형이 있습니다. 이 가이드에서는 양방향, 전환 포리스트 신뢰 관계에 대해 설명합니다. 다음의 간단한 예에서는 두 개의 포리스트(**forest.example.com** 및 **eastforest.example.com**)를 보여줍니다. 각 포리스트의 사용자 및 그룹은 다른 포리스트의 AD에 의해 인증될 수 있습니다. 이렇게 하면 포리스트를 설정할 수 있습니다.

각 도메인에 대해 하나의 영역을 사용하고 각 도메인 컨트롤러에 대해 하나의 디렉토리를 사용하도록 시스템을 설정할 경우, 시스템은 최대 100,000개의 외부 보안 주체(사용자 및 그룹)를 검색할 수 있습니다. 이러한 외부 보안 주체가 다른 영역에서 다운로드한 사용자와 일치하는 경우 액세스 제어 정책에서 사용할 수 있습니다.

액세스 제어 정책에서 사용할 사용자가 없는 도메인에 대해서는 영역을 구성할 필요가 없습니다.

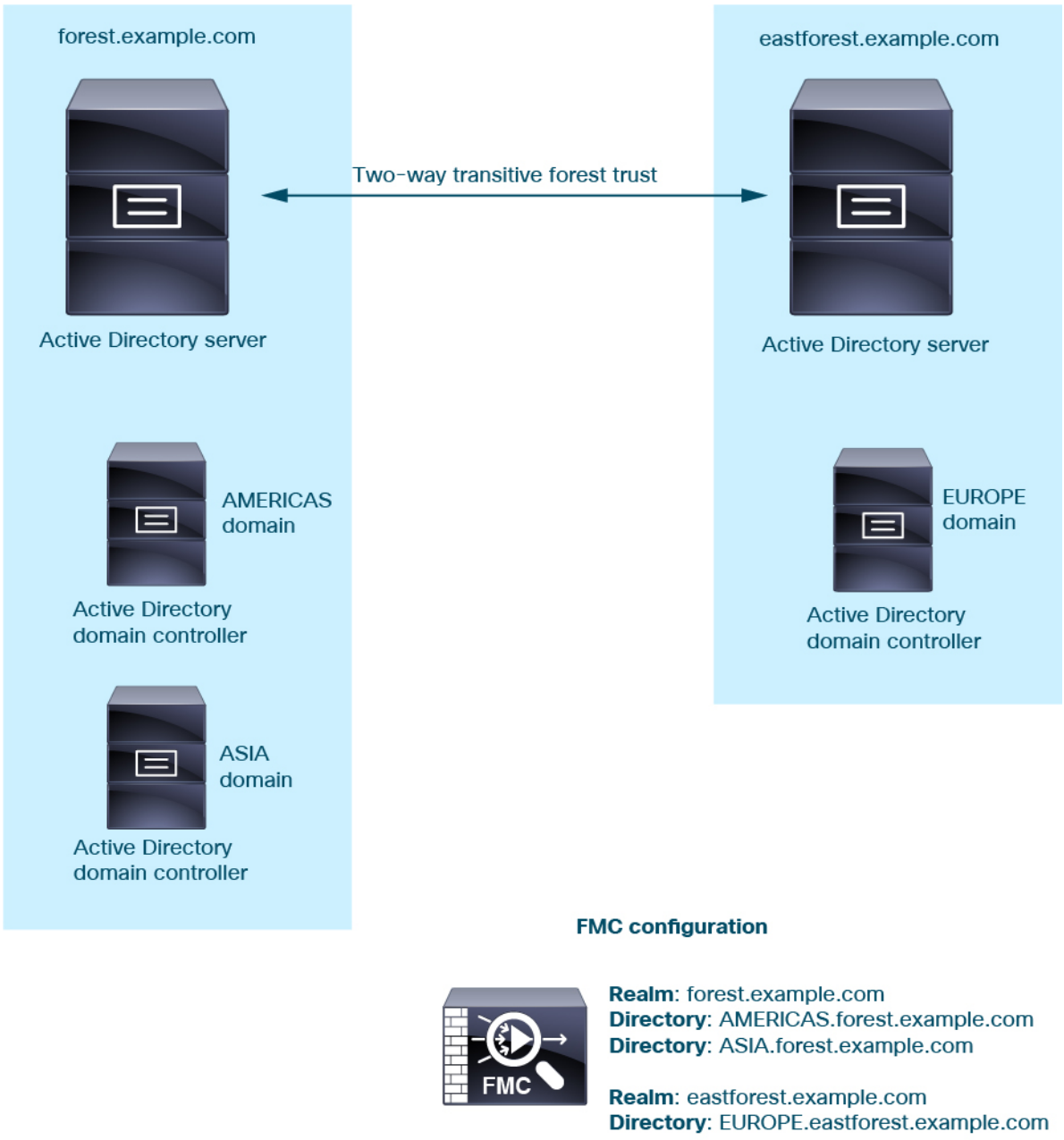


이 예를 계속 진행하려면 AD 포리스트 3개(그중 하나는 하위 도메인 또는 독립적인 포리스트일 수 있음)가 있고, 모두 양방향 전이 포리스트 관계로 설정되어 있다고 가정합니다. 모든 사용자 및 그룹은 3개 포리스트뿐 아니라 시스템에서 사용할 수 있습니다. (위의 예에서와 같이 3개의 AD 도메인을 모두 영역으로 설정하고 모든 도메인 컨트롤러를 해당 영역의 디렉터리로 설정해야 합니다.)



마지막으로 양방향 전이 포리스트 트러스트를 사용하는 2 포리스트 시스템의 사용자 및 그룹에 대해 ID 정책을 적용할 수 있도록 management center를 설정할 수 있습니다. 각 포리스트에 하나 이상의 도메인 컨트롤러가 있으며 각 도메인 컨트롤러가 서로 다른 사용자 및 그룹을 인증한다고 가정해 보겠습니다. management center가 해당 사용자 및 그룹에 대해 ID 정책을 시행할 수 있도록 하려면 관련 사용자를 포함하고 있는 각 도메인을 management center 영역으로, 각 도메인 컨트롤러를 해당 영역의 management center 디렉터리로 설정해야 합니다.

management center를 올바르게 설정하지 못하면 일부 사용자 및 그룹을 정책에서 사용할 수 없습니다. 이 경우 사용자와 그룹을 동기화하려고 할 때 경고가 표시됩니다.



위의 예를 사용하여 다음과 같이 management center를 설정합니다.

- 액세스 제어 정책으로 제어하려는 사용자가 포함된 **forest.example.com**의 도메인에 대한 영역
  - 다음을 위한 영역의 디렉토리 **AMERICAS.forest.example.com**
  - 다음을 위한 영역의 디렉토리 **ASIA.forest.example.com**
- 액세스 제어 정책으로 제어하려는 사용자가 포함된 **eastforest.example.com**의 도메인에 대한 영역

- 다음을 위한 영역의 디렉토리 **EUROPE.eastforest.example.com**

참고 management center는 AD 필드 **msDS-PrincipalName**를 사용하여 각 도메인 컨트롤러에서 사용자 및 그룹 이름을 찾기 위한 참조를 확인합니다. **msDS-PrincipalName**7은(는) NetBIOS 이름을 반환합니다.

영역에 지원되는 서버

다음과 같은 서버 유형에 연결하도록 영역을 구성할 수 있습니다. 단, management center에서 TCP/IP를 통해 이러한 서버에 액세스할 수 있어야 합니다.

서버 유형	**ISE/ISE-PIC** 데이터 검색용으로 지원되는지 여부	**TS** 에이전트 데이터 검색용으로 지원되는지 여부	캡티브 포털 데이터 검색용으로 지원되는지 여부
Windows Server 2012, 2016 및 2019의 Microsoft Active Directory	예	예	예
Microsoft Azure AD	예	아니요	아니요
Linux의 OpenLDAP	아니요	아니요	예

Active Directory 글로벌 카탈로그 서버는 영역 디렉터리로 지원되지 않습니다. 글로벌 카탈로그 서버에 대한 자세한 내용은 Learn.microsoft.com에서 글로벌 카탈로그를 참조하십시오.

참고 TS 에이전트가 다른 패시브 인증 ID 소스(ISE/ISE-PIC)와 공유하는 Microsoft Active Directory Windows Server에 설치된 경우, management center는 TS 에이전트 데이터에 우선순위를 둡니다. TS 에이전트 및 수동 ID 소스가 동일한 IP 주소별로 활동을 보고할 경우, TS 에이전트 데이터만 management center에 로깅됩니다.

서버 그룹 컨피그레이션과 관련하여 다음 사항에 유의하십시오.

- 사용자 그룹 또는 그룹 내의 사용자에 대해 사용자 제어를 수행하려면 LDAP 또는 Active Directory 서버에서 사용자 그룹을 구성해야 합니다.
- 그룹 이름은 LDAP가 내부에서 사용하기 때문에 `s-`로 시작해선 안 됩니다.

  그룹 이름과 조직 단위 이름에는 별표(*), 등호(=), 백슬래시(\) 같은 특수문자가 있으면 안 됩니다. 특수문자가 있으면 해당 그룹이나 조직 단위의 사용자는 다운로드되지 않으며 ID 정책에 사용할 수 없습니다.

- 서버의 하위 그룹 멤버인 사용자를 추가하거나 제외하는 Active Directory 영역을 설정하는 경우, Microsoft는 Windows Server 2012에서 Active Directory의 그룹당 사용자 수가 5,000명 이하일 것을 권장합니다. 자세한 내용은 MSDN의 Active Directory 최대 제한 - 확장성을 참조하십시오.

  필요한 경우 Active Directory 서버 구성을 수정하여 이러한 기본값 제한을 늘리고 더 많은 사용자를 수용할 수 있습니다.

- 원격 데스크탑 서비스 환경의 서버가 보고한 사용자를 고유하게 식별하려면, Cisco TS(Terminal Services) 에이전트를 설정해야 합니다. TS 에이전트를 설치 및 구성하면 개별 사용자에게 고유 포트가 할당되므로, 시스템이 해당 사용자를 고유하게 식별할 수 있습니다. (Microsoft는 *Terminal Services(*터미널 서비스*)*라는 용어를 *Remote Desktop Services(*원격 데스크탑 서비스*)*로 변경했습니다.)

  TS 에이전트에 대한 자세한 내용은 *Cisco TS(Terminal Services)* 에이전트 가이드를 참조하십시오.

지원되는 서버 개체 클래스 및 속성 이름

영역의 서버가 반드시 다음 표에 나와 있는 속성 이름을 사용해야 management center에서 해당 서버의 사용자 메타데이터를 검색합니다. 서버에서 속성 이름이 잘못된 경우 management center에서는 해당 속성의 정보를 데이터베이스에 입력할 수 없습니다.

표 ***1: Secure Firewall Management Center*** 필드에 대한 속성 이름 지도

메타데이터	**Management Center** 특성	**LDAP ObjectClass**	**Active Directory** 속성	**OpenLDAP** 속성
LDAP 사용자 이름	사용자 이름	• user • inetOrgPerson	samaccountname	cn uid
이름	이름		givenname	givenname
성	성		sn	sn
이메일 주소	이메일		mail userprincipalname(메일에 값이 없는 경우)	mail
부서	부서		부서 distinguishedname(부서에 값이 없는 경우)	ou
전화번호	전화번호		telephonenumber	telephonenumber

참고 그룹에 대한 LDAP ObjectClass는 `group`, `groupOfNames`, (`group-of-names` for Active Directory) 또는 `groupOfUniqueNames`입니다.

ObjectClasses 및 속성에 대한 자세한 내용은 다음 참조 자료를 참조하십시오.

- Microsoft Active Directory:
  - ObjectClasses: MSDN의 모든 클래스
  - Attributes: MSDN의 모든 속성
- OpenLDAP: RFC 4512

영역 라이선스 요건

Threat Defense 라이선스

모두

기본 라이선스

제어

영역 요구 사항 및 사전 요건

모델 지원

모두

지원되는 도메인

모두

사용자 역할

- 관리자
- 액세스 관리자
- 네트워크 관리자

Microsoft Azure AD 영역 생성

ISE와 함께 Microsoft Azure AD(Active Directory) 영역을 사용하여 다음 방법 중 하나로 사용자를 인증하고 사용자 제어를 위한 사용자 세션을 가져올 수 있습니다.

- ROPC(Resource Owned Password Credential): 사용자가 사용자 이름 및 비밀번호를 사용하여 AnyConnect와 같은 클라이언트에 로그인할 수 있습니다. ISE는 사용자 세션을 Secure Firewall Management Center로 전송합니다. 자세한 내용은 리소스 소유 비밀번호 자격 증명을 사용하는 Azure AD 및 ISE 정보, 10 페이지을 참고하십시오.

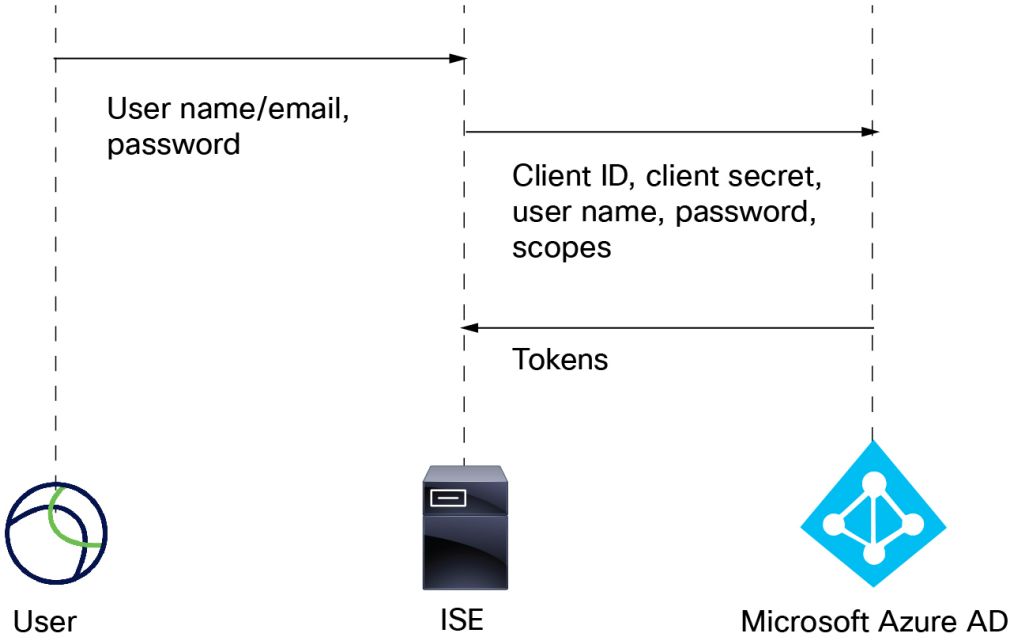
  추가 리소스: Learn.microsoft.com의 Microsoft ID 플랫폼 및 OAuth 2.0 리소스 소유자 비밀번호 자격 증명.

- TEAP(Tunnel-based Extensible Authentication Protocol) 및 TLS(Transport Layer Security)를 사용하는 EAP(Extensible Authentication Protocol) 체이닝, 약식 EAP/TEAP-TLS: TEAP는 보안 터널을 설정하고 해당 보안 터널의 보호 하에 다른 EAP 방법을 실행하는 터널 기반 EAP 방법입니다. ISE는 사용자 자격 증명을 검증하고 사용자 세션을 Secure Firewall Management Center로 전송하는 데 사용됩니다. 자세한 내용은 TEAP/EAP-TLS를 사용하는 Azure AD 및 ISE 정보, 11 페이지를 참고하십시오.

참고 Microsoft Azure AD 영역과 관련된 정책을 구축하기 전에 Microsoft Azure Active Directory 영역에 대한 사용자 제한 항목을 참고하십시오.

리소스 소유 비밀번호 자격 증명을 사용하는 Azure AD 및 ISE 정보

다음 그림에는 ISE 및 ROPC(resource own password credentials)가 있는 Azure AD 영역이 요약되어 있습니다.



ROPC를 사용하면

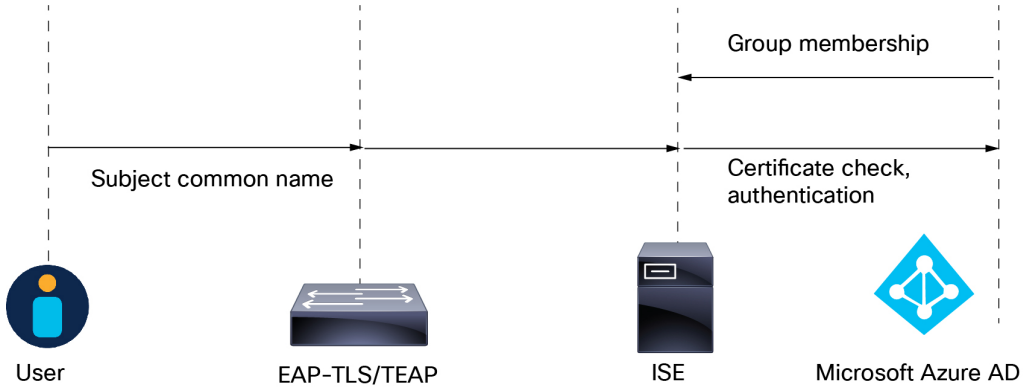
1. 사용자는 AnyConnect와 같은 VPN 클라이언트를 사용하여 사용자 이름(또는 이메일 주소) 및 비밀번호로 로그인합니다.
2. 클라이언트 ID, 클라이언트 암호, 사용자 이름, 비밀번호 및 범위가 Azure AD로 전송됩니다.
3. 토큰은 Azure AD에서 ISE로 전송되며, ISE는 사용자 세션을 Secure Firewall Management Center로 전송합니다.

ISE 구성에 대한 자세한 내용은 Azure Active Directory를 사용하여 ISE 3.0 REST ID 구성을 참조하십시오.

추가 리소스: Learn.microsoft.com의 Microsoft ID 플랫폼 및 OAuth 2.0 리소스 소유자 비밀번호 자격 증명.

TEAP/EAP-TLS를 사용하는 Azure AD 및 ISE 정보

RFC7170에서 정의한 TEAP(Tunnel Extensible Authentication Protocol)는 다음과 같이 ISE 및 Secure Firewall Management Center에서 사용할 수 있습니다.



다음은 Microsoft Azure Active Directory를 사용하여 Cisco ISE 3.2 EAP-TLS 구성을 기반으로 합니다.

1. 사용자의 인증서는 EAP-TLS 또는 EAP-TLS를 내부 방법으로 사용하는 TEAP를 통해 ISE로 전송됩니다.
2. ISE는 사용자의 인증서(유효 기간, 신뢰할 수 있는 인증 기관, 인증서 해지 목록 등)를 평가합니다.
3. ISE는 CN(인증서 주체 이름)을 가져오고 Azure Graph API에 대한 조회를 수행하여 사용자의 그룹 및 기타 특성을 가져옵니다. Azure에서는 이를 UPN(User Principal Name)이라고 합니다.
4. ISE 권한 부여 정책은 Azure에서 반환된 사용자의 속성을 기준으로 평가됩니다.

패시브 인증에 대한 **Microsoft Azure AD** 영역

이 주제에서는 Secure Firewall Management Center에서 패시브 인증을 사용할 영역을 만드는 개략적인 작업에 대해 설명합니다.

프로시저

	명령 또는 동작	목적
단계 **1**	Cisco Secure Dynamic Attributes Connector를 사용하도록 설정합니다.	영역을 사용하려면 Cisco Secure Dynamic Attributes Connector가 필요합니다. 이 작업은 먼저 수행해야 하거나 영역을 생성할 때 활성화할 수도 있습니다. 자세한 내용은 Cisco Secure Dynamic Attributes Connector 활성화를 참조하십시오.
단계 **2**	Microsoft Azure AD를 구성합니다.	이벤트 허브를 설정하고, Microsoft Graph API에 대한 애플리케이션 권한을 부여하고, 감사 로그를 활성화하는 등의 몇 가지 구성 작업이 필요합니다. Microsoft Azure Active Directory 구성, 13 페이지을 참조하십시오.

	명령 또는 동작	목적
단계 **3**	ISE를 구성합니다.	ISE를 구성하는 방법은 사용자가 시스템을 인증하는 방법에 따라 달라집니다. 자세한 내용은 Microsoft Azure AD용 ISE를 구성하는 방법, 15 페이지을 참고하십시오.
단계 **4**	ISE ID 소스를 생성합니다.	ID 소스는 ISE가 Secure Firewall Management Center와 통신할 수 있도록 합니다.
단계 **5**	Microsoft Azure AD 영역을 구성하는 데 필요한 정보를 가져옵니다.	이 정보에는 클라이언트 및 테넌트 ID, 클라이언트 암호 및 Microsoft Azure AD의 기타 정보 저장소가 포함됩니다.
단계 **6**	영역을 구성하고 확인합니다.	액세스 제어 정책에서 사용하기 전에 영역의 구성을 테스트합니다. Azure AD 영역 생성, 17 페이지을 참조하십시오.
단계 **7**	Microsoft Azure AD(SAML) 영역을 사용하여 액세스 제어 정책 및 규칙을 생성합니다.	다른 유형의 영역과 달리 ID 정책을 만들거나 ID 정책을 액세스 제어 정책과 연결할 필요가 없습니다. 기본 액세스 제어 정책 만들기 및 액세스 제어 규칙 생성 및 수정를 참조하십시오.

다음에 수행할 작업

리소스 소유 비밀번호 자격 증명을 사용하는 Azure AD 및 ISE 정보, 10 페이지의 내용을 참조하십시오.

Microsoft Azure Active Directory 구성

이 항목에서는 management center에서 사용할 수 있는 영역으로 Microsoft Azure AD(Active Directory)를 설정하는 방법에 대한 기본 정보를 제공합니다. 이미 Azure AD에 익숙할 것입니다. 그렇지 않은 경우 시작하기 전에 설명서 또는 지원 리소스를 참조하십시오.

애플리케이션에 **Microsoft Graph** 권한 부여

Microsoft 사이트의 권한 부여 및 Microsoft Graph Security API에 설명된 대로 Azure AD 애플리케이션에 Microsoft Graph에 대한 다음 권한을 부여합니다.

- 판독기 역할
- User.Read.All 권한
- Group.Read.All 권한

이 권한이 있으면 management center가 Azure AD에서 사용자 및 그룹을 처음으로 다운로드할 수 있습니다.

management center에서 Azure AD 영역을 설정하기 위한 이 단계의 필수 정보:

- 등록한 앱의 이름
- 애플리케이션(클라이언트) **ID**
- 클라이언트 비밀번)
- 디렉터리(테넌트) **ID**

이벤트 허브 설정

Microsoft 사이트에서 빠른 시작: Azure 포털을 사용하여 이벤트 허브 생성에 설명된 대로 이벤트 허브를 설정합니다. management center는 이벤트 허브 감사 로그를 사용하여 사용자 및 그룹에 대한 정기 업데이트를 다운로드합니다.

추가 정보: Azure Event Hubs의 기능 및 용어

중요 **Standard(**표준**)** 가격 책정 계층 이상을 선택해야 합니다. **Basic(**기본**)**을 선택하면 영역을 사용할 수 없습니다.

management center에서 Azure AD 영역을 설정하기 위한 이 단계의 필수 정보:

- 네임스페이스 이름
- 연결 문자열 - 기본 키
- 이벤트 허브 이름

  Azure AD 영역을 설정할 때 이 이름에 포트(**:9093**)를 추가해야 합니다.
- 소비자 그룹 이름

감사 로그 활성화

자습서: Microsoft 사이트의 Azure 이벤트 허브에 Azure Active Directory 로그 스트리밍에 설명된 대로 감사 로그를 활성화합니다.

Azure AD용 ISE 구성

사용자 세션 정보를 management center로 전송하려면 Azure Active Directory를 사용하여 ISE 3.0 REST ID 구성에 설명된 대로 Azure AD용 ISE를 구성합니다.

향후 작업

Microsoft Azure AD용 ISE를 구성하는 방법, 15 페이지의 내용을 참조하십시오.

Microsoft Azure AD용 ISE를 구성하는 방법

Microsoft Azure AD 영역에서는 사용자 세션(로그인, 로그아웃)을 management center로 전송하는 것이 ISE의 책임입니다. 이 항목에서는 Azure AD 영역에서 사용하기 위해 ISE를 설정하는 방법을 설명합니다.

리소스 소유 비밀번호 자격 증명 인증

ROPC(Resource Owner Password Credentials)를 사용하여 REST(Representational State Transfer) ID 서비스를 통해 구현된 Microsoft Azure AD에서 ISE를 사용하려면 Azure Active Directory를 사용하여 ISE 3.0 REST ID 구성을 참조하십시오.

TEAP/EAP-TLS

인증 프로토콜로 EAP-TLS 또는 TEAP를 사용하는 Azure AD 그룹 멤버십 및 기타 사용자 속성을 기반으로 하는 권한 부여 정책과 함께 ISE를 사용하려면 Azure Active Directory를 사용하여 Cisco ISE 3.2 EAP-TLS 구성을 참고하십시오.

향후 작업

Microsoft Azure AD 영역에 대한 필수 정보 가져오기, 15 페이지

Microsoft Azure AD 영역에 대한 필수 정보 가져오기

이 작업에서는 management center에서 Microsoft Azure AD 영역을 설정하는 데 필요한 정보를 가져오는 방법을 설명합니다. Microsoft Azure Active Directory 구성, 13 페이지에 설명된 대로 Microsoft Azure AD를 설정할 때 이 정보를 이미 얻었을 수 있습니다.

프로시저

단계 **1** 최소한 제품 디자이너 역할의 사용자로 https://portal.azure.com/에 로그인합니다.

단계 **2** 페이지 상단에서 **Mictosoft Entra ID**를 클릭합니다.

단계 **3** 왼쪽 열에서 **App Registrations(**앱 등록**)**를 클릭합니다.

단계 **4** 필요한 경우 표시된 앱 목록을 필터링하여 사용할 앱을 표시합니다.

단계 **5** 앱의 이름을 클릭합니다.

단계 **6** 이 페이지에서 다음 값 옆에 있는 **Copy(**복사**)** ( )을 클릭하고 해당 값을 텍스트 파일에 붙여 넣습니다.

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

단계 **7** **Client Credentials(**클라이언트 인증서**)**를 클릭합니다.

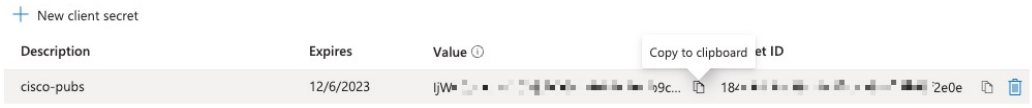
단계 **8** 클라이언트 비밀번호 값(클라이언트 비밀번호 *ID*가 아님)을 이미 알고 있는 경우가 아니라면 다음과 같이 새 클라이언트 비밀번호를 만들어야 합니다.

a) **New Client Secret(**새 클라이언트 비밀번호**)**을 클릭합니다.

b) 제공된 필드에 필수 정보를 입력합니다.

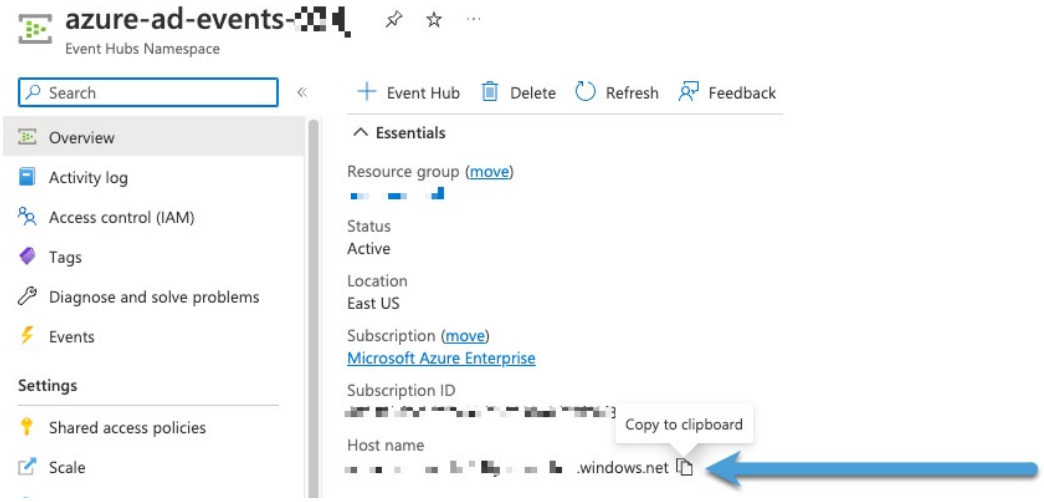
c) **Add(**추가**)**를 클릭합니다.

d) 다음 그림과 같이 Value(값) 옆의 **Copy(**복사**)** ( )을 클릭합니다.



단계 **9** https://portal.azure.com/에서 **Event Hubs** > **(**이벤트 허브의 이름**)**을 클릭합니다.

단계 **10** 오른쪽 창에서 클립보드의 **Host name(**호스트 이름**)** 값 옆에 있는 **Copy(**복사**)** ( )을 클릭하고 값을 클립보드에 붙여 넣습니다. 이는 이벤트 허브 호스트 이름입니다.

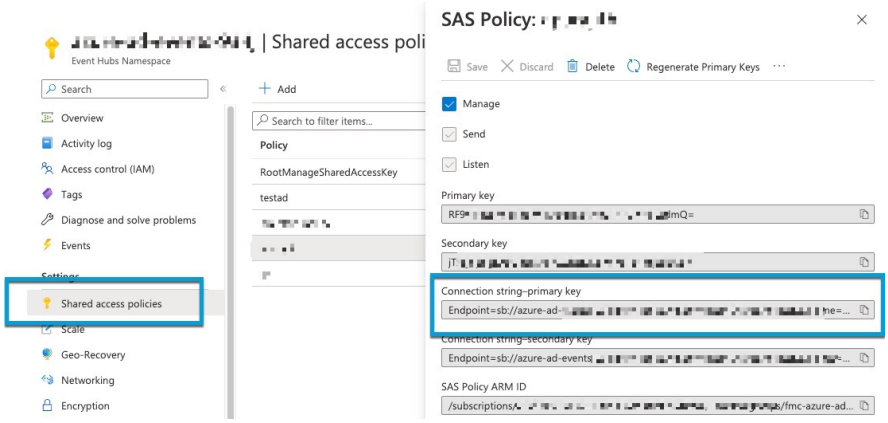


단계 **11** 이벤트 허브의 이름을 텍스트 파일에 기록하거나 복사합니다(페이지 상단의 이벤트 허브 네임스페이스와 동일).

단계 **12** 왼쪽 창의 Settings(설정) 아래에서 **Shared access policies(**공유 액세스 정책**)**를 클릭합니다.

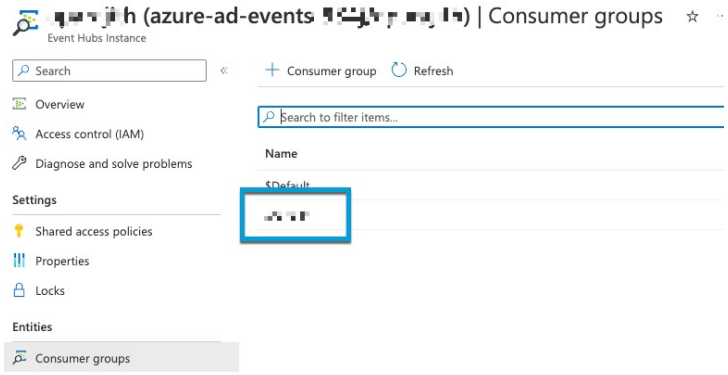
단계 **13** 정책 이름을 클릭합니다.

단계 **14** **Connection string-primary key(**연결 문자열 기본 키**)** 옆에 있는 **Copy(**복사**)** ( )을 클릭합니다.



단계 **15** **Overview(**개요**)** > **Entities(**엔터티**)** > **Event Hubs(**이벤트 허브**)** > **(**이벤트 허브의 이름**)** > **Entities(**엔터티**)** > **Consumer Groups(**소비자 그룹**)**를 클릭합니다.

다음 값을 기록하거나 클립보드에 복사합니다. 이는 소비자 그룹 이름입니다.



단계 **16** 왼쪽 창에서 **Overview(**개요**)**를 클릭합니다.

단계 **17** **Namespace(**네임스페이스**)** 옆에 있는 **Copy(**복사**)** ( )을 클릭합니다.

이는 이벤트 허브 주제 이름입니다.

Azure AD 영역 생성

다음 절차에 따라 영역(management center와 Microsoft Azure AD 영역 간의 연결)을 생성할 수 있습니다.

시작하기 전에

다음 작업을 모두 완료합니다.

- Microsoft Azure AD용 ISE를 구성하는 방법, 15 페이지에 설명된 대로 ISE 구성
- ISE/ISE-PIC 구성에 설명된 대로 ISE ID 소스 생성
- Cisco Secure Dynamic Attributes Connector 활성화에 설명된 대로 Cisco Secure Dynamic Attributes Connector를 활성화합니다.
- Microsoft Azure AD 영역에 대한 필수 정보 가져오기, 15 페이지에 설명된 대로 Azure AD 영역에 필요한 값을 가져옵니다.
- Microsoft Azure Active Directory 구성, 13 페이지에 설명된 대로 Azure AD 구성

참고 Azure AD 영역을 사용하여 사용자 및 ID 제어를 수행하려면 연결된 Azure AD 영역이 있는 액세스 제어 정책만 필요합니다. ID 정책을 생성할 필요가 없습니다.

프로시저

단계 **1** Secure Firewall Management Center에 로그인합니다.

단계 **2** **Integration(**통합**)** > **Other Integrations(**기타 통합**)** > **Realms(**영역**)** 버튼을 클릭합니다.

단계 **3** 새 영역을 생성하려면 **Add Realm(**영역 추가**)** > **Azure AD**를 클릭합니다.

단계 **4** 다음 정보를 입력합니다.

항목	설명
이름	
(선택 사항). 설명	
클라이언트 **ID**	Microsoft Azure AD 영역에 대한 필수 정보 가져오기, 15 페이지에서 설명한 대로 찾은 정보를 입력합니다.
Client Secret(클라이언트 비밀번호**)**	
테넌트 **ID**	
이벤트 허브 호스트 이름	
이벤트 허브 이름	
이벤트 허브 연결 문자열	

항목	설명
(선택 사항). 제외된 사용자 그룹	ID 제어를 위해 사용자를 다운로드하지 않을 그룹을 하나 이상 입력합니다. 이 그룹의 사용자는 액세스 제어 정책에서 사용할 수 없습니다. 한 줄에 하나의 그룹 이름을 입력하고 그 뒤에 줄바꿈을 입력합니다. 그룹 이름은 대소문자를 구분합니다.

단계 **5** 다른 작업(영역 활성화, 비활성화, 삭제 등)을 수행하는 방법은 영역 관리, 43 페이지 섹션을 참조하십시오.

단계 **6** Microsoft Azure AD 영역에 대한 필수 정보 가져오기, 15 페이지에서 설명한 대로 찾은 값을 입력합니다.

단계 **7** **Test(**테스트**)**를 클릭합니다.

단계 **8** 테스트에 표시되는 오류를 수정합니다.

단계 **9** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

기본 액세스 제어 정책 만들기에 설명된 대로 액세스 제어 정책 및 규칙을 생성합니다.

참고 Microsoft Azure AD 영역과 관련된 정책을 구축하기 전에 Microsoft Azure Active Directory 영역에 대한 사용자 제한 항목을 참고하십시오.

Azure AD 사용자 세션 시간 초과

ISE/ISE-PIC에 대한 Azure AD 사용자 세션 시간 초과는 Azure AD 영역을 편집할 때 **User Session Timeout(**사용자 세션 시간 초과**)** 페이지에서 사용할 수 있습니다.

기본값은 1440분(24시간)입니다. 시간이 초과되면 사용자의 세션은 종료됩니다. 사용자가 다시 로그인하지 않고 계속 액세스하면, 해당 사용자는 management center가 Unknown(알 수 없음)으로 간주합니다(**Failed Captive Portal Users(**실패한 캡티브 포털 사용자**)** 제외).

LDAP 영역 또는 Active Directory 영역 및 영역 디렉터리 생성

영역 없이 ISE/ISE-PIC를 설정하는 경우에는 Secure Firewall Management Center로 사용자가 표시되는 방식에 영향을 주는 사용자 세션 시간 초과가 있다는 점에 유의하십시오. 자세한 내용은 영역 필드, 23 페이지를 참조하십시오.

다음 절차를 수행하면 영역(management center와 Active Directory 영역 간 연결) 및 디렉터리(management center와 LDAP 서버 또는 Active Directory 도메인 컨트롤러 간 연결)를 만들 수 있습니다.

(권장) management center에서 Active Directory 서버로 안전하게 연결하려면 먼저 다음 작업을 수행합니다.

- Active Directory 서버의 루트 인증서 내보내기, 31 페이지
- Active Directory 서버 이름 찾기, 30 페이지

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

영역 디렉터리 설정 필드에 대한 자세한 내용은 영역 필드, 23 페이지 및 영역 디렉터리 및 동기화 필드, 27 페이지의 내용을 참조하십시오.

도메인 간 신뢰를 사용하여 영역을 설정하는 단계별 예가 도메인 간 신뢰를 위한 Management Center 구성: 설정, 35 페이지에 나와 있습니다.

Active Directory 글로벌 카탈로그 서버는 영역 디렉터리로 지원되지 않습니다. 글로벌 카탈로그 서버에 대한 자세한 내용은 Learn.microsoft.com에서 글로벌 카탈로그를 참조하십시오.

참고 모든 Microsoft Active Directory(AD) 영역에 대한 고유 **AD Primary Domain(AD** 기본 도메인**)**을 지정해야 합니다. 다른 Microsoft AD 영역에 동일한 **AD Primary Domain(AD** 기본 도메인**)**을 지정할 수는 있지만, 시스템이 제대로 작동하지 않습니다. 이러한 상황이 발생하는 이유는 시스템이 고유 ID를 각 영역에 있는 모든 사용자에게 할당하기 때문입니다. 따라서 시스템은 특정 사용자 또는 그룹을 확실히 식별할 수 없습니다. 시스템에서 사용자와 그룹을 적절히 식별하지 못하기 때문에 **AD Primary Domain(AD** 기본 도메인**)**이 동일한 영역 하나 이상을 지정할 수 없습니다. 이러한 상황이 발생하는 이유는 시스템이 고유 ID를 각 영역에 있는 모든 사용자에게 할당하기 때문입니다. 따라서 시스템은 특정 사용자 또는 그룹을 확실히 식별할 수 없습니다.

영역 없이 ISE/ISE-PIC를 설정하는 경우에는 Secure Firewall Management Center로 사용자가 표시되는 방식에 영향을 주는 사용자 세션 시간 초과가 있다는 점에 유의하십시오. 자세한 내용은 영역 필드, 23 페이지를 참조하십시오.

시작하기 전에

캡티브 포털(captive portal)에 Kerberos 인증을 사용하는 경우 시작하기 전에 다음 섹션을 참조하십시오.Kerberos 인증 사전 요건, 22 페이지

참고 Microsoft Azure Active Directory는 캡티브 포털을 지원하지 않습니다.

중요 Secure Firewall Management Center와 Active Directory 도메인 컨트롤러 간의 레이턴시를 줄이려면 Secure Firewall Management Center와 최대한 지리적으로 가까운 영역 디렉터리(즉, 도메인 컨트롤러)를 구성하는 것이 좋습니다.

예를 들어 Secure Firewall Management Center가 북미에 있는 경우 북미에도 있는 영역 디렉터리를 구성합니다. 그렇지 않으면 사용자 및 그룹 다운로드 시간 초과 등의 문제가 발생할 수 있습니다.

프로시저

단계 **1** Secure Firewall Management Center에 로그인합니다.

단계 **2** **Integration(**통합**)** > **Other Integrations(**기타 통합**)** > **Realms(**영역**)** 버튼을 클릭합니다.

단계 **3** 새 영역을 생성하려면 **Add Realm(**영역 추가**)** 드롭다운 목록에서 선택합니다.

단계 **4** 다른 작업(영역 활성화, 비활성화, 삭제 등)을 수행하는 방법은 영역 관리, 43 페이지 섹션을 참조하십시오.

단계 **5** 영역 필드, 23 페이지에 설명된 대로 영역 정보를 입력합니다.

단계 **6** Directory Server Configuration(디렉터리 서버 구성) 섹션에서 영역 디렉터리 및 동기화 필드, 27 페이지에 설명된 대로 디렉터리 정보를 입력합니다.

단계 **7** (선택 사항). 이 영역에 대해 다른 도메인을 설정하려면 **Add another directory(**다른 디렉토리 추가**)**를 클릭합니다.

단계 **8** **Configure Groups and Users(**그룹 및 사용자 설정**)**를 클릭합니다.
다음 정보를 입력합니다.

정보	설명
AD Primary Domain(AD 기본 도메인**)**	사용자가 인증해야 하는 Active Directory 서버의 도메인입니다. 추가 정보는 영역 필드, 23 페이지 내용을 참조하십시오.
Base DN(기본 **DN)**	Secure Firewall Management Center이 사용자 데이터 검색을 시작해야 하는 서버의 디렉토리 트리입니다.
Group DN(그룹 **DN)**	Secure Firewall Management Center이 그룹 데이터 검색을 시작해야 하는 서버의 디렉토리 트리입니다.
그룹 로드	Active Directory 서버에서 로컬 그룹을 로드하려면 클릭합니다. 그룹이 표시되지 않으면 **AD Primary Domain(**기본 도메인**)**, **Base DN(**기본 **DN)** 및 **Group DN(**그룹 **DN)** 필드에 정보를 입력하거나 편집하고 **Load Groups(**그룹 로드**)**를 클릭합니다. 필드에 대한 내용은 영역 필드, 23 페이지의 내용을 참조하십시오.

정보	설명
사용 가능한 그룹 섹션	정책에서 사용할 그룹을 **Included Groups and Users(**포함된 그룹 및 사용자**)** 또는 **Excluded Groups and Users(**제외된 그룹 및 사용자**)** 목록으로 이동하여 제한합니다. 예를 들어 한 그룹을 **Included Groups and Users(**포함된 그룹 및 사용자**)** 목록으로 이동하면 해당 그룹만 정책에 사용할 수 있고 다른 모든 그룹은 제외됩니다. **Excluded Groups and Users(**제외된 그룹 및 사용자**)**의 그룹과 여기에 포함된 사용자는 사용자 인식 및 제어에서 제외됩니다. 다른 모든 그룹 및 사용자는 사용할 수 있습니다. 자세한 내용은 영역 디렉터리 및 동기화 필드, 27 페이지를 참고하십시오.

단계 **9** **Realm Configuration(**영역 설정**)** 탭을 클릭합니다.

단계 **10** **Group Attribute(**그룹 속성**)**를 입력하고 (캡티브 포털에 Kerberos 인증을 사용하는 경우) **AD Join Username(AD** 조인 사용자 이름**)** 및 **AD Join Password(AD** 조인 암호**)**를 입력합니다. 자세한 내용은 영역 디렉터리 및 동기화 필드, 27 페이지를 참고하십시오.

단계 **11** Kerberos 인증을 사용하는 경우 **Test(**테스트**)**를 클릭합니다. 테스트가 실패하면 잠시 기다렸다가 다시 시도하십시오.

단계 **12** **ISE/ISE-PIC Users(ISE/ISE-PIC** 사용자**)**, **Terminal Server Agent Users(**터미널 서버 에이전트 사용자**)**, **Captive Portal Users(**캡티브 포털 사용자**)**, **Failed Captive Portal Users(**실패한 캡티브 포털 사용자**)** 및 **Guest Captive Portal Users(**게스트 캡티브 포털 사용자**)**에 대한 사용자 세션 시간 초과 값을 분 단위로 입력합니다.

단계 **13** 영역 설정을 완료했으면 **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 도메인 간 신뢰를 위한 Management Center 구성: 설정, 35 페이지
- 사용자 및 그룹 동기화, 33 페이지
- 영역을 편집, 삭제, 활성화 또는 비활성화합니다(영역 관리, 43 페이지 참조).
- 영역 비교, 44 페이지에 전달하는 고성능 고속 어플라이언스입니다.
- 필요한 경우 작업 상태를 모니터링합니다. Cisco Secure Firewall Management Center 관리 가이드의 작업 메시지 보기를 참조하십시오.

Kerberos 인증 사전 요건

Kerberos를 사용하여 캡티브 포털(captive portal) 사용자를 인증하는 경우 다음 사항에 유의하십시오.

호스트 이름 문자 제한

Kerberos 인증을 사용하는 경우 매니지드 디바이스의 호스트 이름은 15자 미만이어야 합니다(Windows에서 설정한 NetBIOS 제한). 그렇지 않으면 캡티브 포털 인증이 실패합니다. 디바이스를 설정할 때 매니지드 디바이스 호스트 이름을 설정합니다. 자세한 내용은 Microsoft 설명서 사이트에서 컴퓨터, 도메인, 사이트 및 OU에 대한 Active Directory의 명명 규칙과 유사한 문서를 참조하십시오.

DNS 응답 문자 제한

DNS는 호스트 이름에 대해 64KB 이하의 응답을 반환해야 합니다. 그렇지 않으면 AD 연결 테스트가 실패합니다. 이 제한은 양방향으로 적용되며 RFC 6891 섹션-6.2.5에 설명되어 있습니다.

영역 필드

다음 필드는 영역을 구성하는 데 사용됩니다.

영역 컨피그레이션 필드

이러한 설정은 영역의 모든 Active Directory 서버 또는 (디렉터리라고도 하는) 도메인 컨트롤러에 적용됩니다.

이름

영역의 고유한 이름입니다.

- ID 정책에 영역을 사용하려는 경우, 시스템은 영숫자 및 특수 문자를 지원합니다.
- RA VPN 설정에서 영역을 사용하려는 경우, 시스템에서는 영숫자와 하이픈(-), 밑줄(_), 더하기(+) 문자를 지원합니다.

설명

(선택 사항). 영역에 대한 설명을 입력합니다.

유형

영역의 유형으로, Microsoft Active Directory의 경우에는 **AD**이며 다른 지원되는 저장소의 경우에는 **LDAP** 또는 **Local(**로컬**)**입니다. 지원되는 LDAP 저장소 목록은 영역에 지원되는 서버, 7 페이지 섹션을 참조하십시오. LDAP 리포지토리를 사용하여 캡티브 포털 사용자를 인증할 수 있습니다. 다른 모든 경우에는 Active Directory가 필요합니다.

참고 캡티브 포털만 LDAP 영역을 지원합니다.

영역 유형 **LOCAL**은 로컬 사용자 설정을 설정하는 데 사용됩니다. LOCAL 영역은 원격 액세스 사용자 인증에 사용됩니다.

LOCAL 영역에 대해 다음 로컬 사용자 정보를 추가합니다.

- **Username(**사용자 이름**)** - 로컬 사용자의 이름입니다.
- **Password(**암호**)**—로컬 사용자 암호입니다.

- **Confirm Password(**암호 확인**) -** 로컬 사용자 암호를 확인합니다.

참고 LOCAL 영역에 사용자를 더 추가하려면 **Add another local user(**다른 로컬 사용자 추가**)**를 클릭합니다.

영역을 생성한 후 사용자를 추가하고 로컬 사용자의 암호를 업데이트할 수 있습니다. 여러 LOCAL 영역을 생성할 수도 있지만 비활성화할 수는 없습니다.

AD Primary Domain(AD 기본 도메인**)**

Microsoft Active Directory 영역에만 해당됩니다. 사용자가 인증해야 하는 Active Directory 서버의 도메인입니다.

참고 모든 Microsoft Active Directory(AD) 영역에 대한 고유 **AD Primary Domain(AD** 기본 도메인**)**을 지정해야 합니다. 다른 Microsoft AD 영역에 동일한 **AD Primary Domain(AD** 기본 도메인**)**을 지정할 수는 있지만, 시스템이 제대로 작동하지 않습니다. 이러한 상황이 발생하는 이유는 시스템이 고유 ID를 각 영역에 있는 모든 사용자에게 할당하기 때문입니다. 따라서 시스템은 특정 사용자 또는 그룹을 확실히 식별할 수 없습니다. 시스템에서 사용자와 그룹을 적절히 식별하지 못하기 때문에 **AD Primary Domain(AD** 기본 도메인**)**이 동일한 영역 하나 이상을 지정할 수 없습니다. 이러한 상황이 발생하는 이유는 시스템이 고유 ID를 각 영역에 있는 모든 사용자에게 할당하기 때문입니다. 따라서 시스템은 특정 사용자 또는 그룹을 확실히 식별할 수 없습니다.

AD Join Username(AD 죠인 사용자 이름**)** 및 **AD Join Password(AD** 죠인 비밀번호**)**
(영역을 편집 할 때 **Realm Configuration(**영역 설정**)** 탭 페이지에서 사용할 수 있습니다.)

Kerberos 캡티브 포털 액티브 인증을 위한 Microsoft Active Directory 영역으로, Active Directory 도메인에서 도메인 컴퓨터 계정을 생성할 권한이 있는 모든 Active Directory 사용자의 고유 사용자 이름 및 비밀번호입니다.

다음에 유의해야 합니다.

- DNS는 Active Directory 도메인 컨트롤러의 IP 주소에 대한 도메인 이름을 확인할 수 있어야 합니다.
- 지정하는 사용자는 컴퓨터를 Active Directory 도메인에 가입시킬 수 있어야 합니다.
- 사용자 이름은 온전한 이름이어야 합니다(예: **`administrator`**)가 아닌 **`administrator@mydomain.com`**.

`Kerberos`(Kerberos를 옵션으로 사용하려는 경우에는 **`HTTP Negotiate(HTTP 협상)`**)를 ID 규칙의 **Authentication Protocol(**인증 프로토콜**)**로 선택하는 경우, Kerberos 캡티브 포털 액티브 인증을 수행하려면 **AD Join Username(AD** 죠인 사용자 이름**)**과 **AD Join Password(AD** 죠인 비밀번호**)**를 사용하여 선택한 **Realm(**영역**)**을 구성해야 합니다.

참고 SHA-1 해시 알고리즘은 Active Directory 서버에 암호를 저장하는 데 안전하지 않으므로 사용할 수 없습니다. 자세한 내용은 Microsoft TechNet의 SHA1에서 SHA2로 인증 기관 해싱 알고리즘 마이그레이션 또는 오픈 웹 애플리케이션 보안 프로젝트 웹 사이트의 암호 스토리지 치트 시트와 같은 참조를 참조하십시오.

Active Directory와의 통신에는 SHA-256을 사용하는 것이 좋습니다.

Directory Username and Directory Password(디렉토리 사용자 이름 및 디렉토리 비밀번호**)**

검색하려는 사용자 정보에 대한 적절한 액세스 권한이 있는 사용자의 고유 사용자 이름 및 비밀번호입니다.

다음에 유의하십시오.

- 일부 Microsoft Active Directory 버전의 경우 사용자 및 그룹을 읽기 위해 특정 권한이 필요할 수 있습니다. 자세한 내용은 Microsoft Active Directory와 함께 제공되는 설명서를 참조하십시오.
- OpenLDAP의 경우 사용자의 액세스 권한은 OpenLDAP 사양 섹션 8에서 설명하는 `<level>` 파라미터에 의해 결정됩니다. 사용자의 `<level>`은 `auth` 이상이어야 합니다.
- 사용자 이름은 완전 해야 합니다 (예: **`administrator@mydomain.com`**, 관리자 아님).

참고 SHA-1 해시 알고리즘은 Active Directory 서버에 암호를 저장하는 데 안전하지 않으므로 사용할 수 없습니다. 자세한 내용은 Microsoft TechNet의 SHA1에서 SHA2로 인증 기관 해싱 알고리즘 마이그레이션 또는 오픈 웹 애플리케이션 보안 프로젝트 웹 사이트의 암호 스토리지 치트 시트와 같은 참조를 참조하십시오.

Active Directory와의 통신에는 SHA-256을 사용하는 것이 좋습니다.

Base DN(기본 **DN)**

(선택 사항) Secure Firewall Management Center이 사용자 데이터 검색을 시작해야 하는 서버의 디렉토리 트리입니다. **Base DN(**기본 **DN)**을 지정하지 않으면 시스템은 서버에 연결할 수 있는 경우 최상위 DN을 검색합니다.

일반적으로, 기본 DN(distinguished name)은 회사 도메인 이름 및 운영 단위를 나타내는 기본 구조를 가지고 있습니다. 예를 들어, 예시 회사의 보안 조직은 **`ou=security,dc=example,dc=com`**의 기본 DN을 가질 수 있습니다.

Group DN(그룹 **DN)**

(선택 사항) Secure Firewall Management Center이 그룹 속성으로 사용자를 검색해야 하는 서버의 디렉토리 트리입니다. 지원되는 그룹 속성 목록은 지원되는 서버 개체 클래스 및 속성 이름, 8 페이지에서 확인할 수 있습니다. **Group DN(**그룹 **DN)**을 지정하지 않으면 시스템은 서버에 연결할 수 있는 경우 최상위 DN을 검색합니다.

참고 다음은 디렉토리 서버의 사용자, 그룹, DN에서 시스테이 지원하는 문자의 목록입니다. 다음 이외의 문자를 사용하면 시스템에서 사용자 및 그룹을 다운로드하지 못할 수 있습니다.

엔티티	지원되는 문자
사용자 이름	**a-z A-Z 0-9 ! # $ % ^ & ( ) _ - { } ' . ~ `**
그룹 이름	**a-z A-Z 0-9 ! # $ % ^ & ( ) _ - { } ' . ~ `**
기본 DN 및 그룹 DN	**a-z A-Z 0-9 ! @ $ % ^ & * ( ) _ - . ~ `**

사용자 이름의 끝 부분을 포함하여 공백은 지원되지 않습니다.

아래 필드는 기존 영역을 편집할 때만 사용할 수 있습니다.

사용자 세션 시간 초과

(영역을 편집 할 때 **Realm Configuration(**영역 설정**)** 탭 페이지에서 사용할 수 있습니다.)

사용자 세션이 시간 초과될 때까지의 시간을 분 단위로 입력합니다. 기본값은 사용자 로그인 이벤트 후 1,440(24시간)입니다. 시간이 초과되면 사용자의 세션은 종료됩니다. 사용자가 다시 로그인하지 않고 계속 액세스하면, 해당 사용자는 management center가 Unknown(알 수 없음)으로 간주합니다(**Failed Captive Portal Users(**실패한 캡티브 포털 사용자**)** 제외).

또한 영역 없이 ISE/ISE-PIC를 설정하고 시간 초과가 초과된 경우에는 해결 방법이 필요합니다. 자세한 내용은 Cisco TAC에 문의하십시오.

다음에 대한 시간 초과 값을 설정할 수 있습니다.

- 사용자 에이전트 및 **ISE/ISE-PIC** 사용자: 사용자 에이전트 또는 ISE/ISE-PIC가 추적하는 사용자의 시간 초과 값으로, 패시브 인증의 유형입니다.

  지정하는 시간 초과 값은 pxGrid SXP 세션 주제 구독(예: 대상 SGT 매핑)에 적용되지 않습니다. 대신 ISE에서 지정된 매핑에 대한 삭제 또는 업데이트 메시지가 없는 한 세션 주제 매핑이 유지됩니다.

  ISE/ISE-PIC에 대한 자세한 내용은 ISE/ISE-PIC ID 소스의 내용을 참조하십시오.

- 터미널 서비스 에이전트 사용자: TS 에이전트가 추적하는 사용자의 시간 초과 값으로, 패시브 인증의 유형입니다. 자세한 내용은 TS(Terminal Services) 에이전트 ID 소스를 참고하십시오.

- 캡티브 포털 사용자: 캡티브 포털을 이용해 무사히 로그인한 사용자의 시간 초과 값으로, 액티브 인증의 유형입니다. 자세한 내용은 캡티브 포털 ID 소스를 참고하십시오.

- 실패한 캡티브 포털 사용자: 캡티브 포털을 사용하여 무사히 로그인하지 못한 사용자의 시간 초과 값입니다. management center가 사용자를 Failed Auth User(실패한 인증 사용자)로 간주하기 전의 최대 로그인 시도 횟수를 설정할 수 있습니다. Failed Auth User(실패한 인증 사용자)는 액세스 컨트롤 정책을 이용해 네트워크에 대한 액세스를 받을 수 있으며, 이 경우 이 시간 초과 값이 해당 사용자에게 적용됩니다.

캡티브 포털 로그인에 대한 자세한 내용은 캡티브 포털(captive portal) 필드 섹션을 참조하십시오.

- 게스트 캡티브 포털 사용자: 게스트 사용자로 캡티브 포털에 로그인한 사용자의 시간 초과 값입니다. 자세한 내용은 캡티브 포털 ID 소스를 참고하십시오.

영역 디렉터리 및 동기화 필드

영역 디렉토리 필드

이러한 설정은 영역의 개별 서버(Active Directory 도메인 컨트롤러 등)에 적용됩니다.

Hostname / IP Address(호스트 이름**/IP** 주소**)**

Active Directory 도메인 컨트롤러 시스템의 정규화된 호스트 이름입니다. 정규화된 이름을 찾으려면 Active Directory 서버 이름 찾기, 30 페이지의 내용을 참조하십시오.

캡티브 포털을 인증하는 데 Kerberos를 사용하는 경우 다음 사항도 이해해야 합니다.

Kerberos 인증을 사용하는 경우 매니지드 디바이스의 호스트 이름은 15자 미만이어야 합니다(Windows에서 설정한 NetBIOS 제한). 그렇지 않으면 캡티브 포털 인증이 실패합니다. 디바이스를 설정할 때 매니지드 디바이스 호스트 이름을 설정합니다. 자세한 내용은 Microsoft 설명서 사이트에서 컴퓨터, 도메인, 사이트 및 OU에 대한 Active Directory의 명명 규칙과 유사한 문서를 참조하십시오.

DNS는 호스트 이름에 대해 64KB 이하의 응답을 반환해야 합니다. 그렇지 않으면 AD 연결 테스트가 실패합니다. 이 제한은 양방향으로 적용되며 RFC 6891 섹션-6.2.5에 설명되어 있습니다.

Port(포트**)**

서버의 포트입니다.

암호화

(적극 권장함.) 사용할 암호화 방법:

- **`STARTTLS`** — 암호화된 LDAP 연결
- **`LDAPS`** — 암호화된 LDAP 연결
- **`None`(없음)** — 암호화되지 않은 LDAP 연결(안전하지 않은 트래픽)

Active Directory 서버와 안전하게 통신하려면 Active Directory에 안전하게 연결, 30 페이지의 내용을 참조하십시오.

CA 인증서

서버에 인증하는 데 사용할 TLS/SSL 인증서입니다. TLS/SSL 인증서를 사용하려면 **`STARTTLS`** 또는 **`LDAPS`**를 **Encryption(**암호화**)** 유형으로 구성해야 합니다.

인증서를 사용하여 인증하는 경우에는 인증서의 서버 이름이 서버 **Hostname / IP Address(**호스트 이름**/IP** 주소**)**와 일치해야 합니다. 예를 들어 IP 주소로 10.10.10.250을 사용하는데 인증서에서 **`computer1.example.com`**을 사용하면, 연결이 실패합니다.

디렉토리 서버에 연결하는 데 사용된 인터페이스

Secure Firewall Threat Defense에서 Active Directory 서버에 안전하게 연결할 수 있도록 RA VPN 인증에만 필요합니다. 그러나 이 인터페이스는 사용자와 그룹을 다운로드하는 데 사용되지 않습니다.

라우팅 인터페이스 그룹만 선택할 수 있습니다. 자세한 내용은 Interface(인터페이스)를 참고하십시오.

다음 중 하나를 클릭합니다.

- **Resolve via route lookup(**경로 조회를 통해 확인**)**: 라우팅을 사용하여 Active Directory 서버에 연결합니다.
- **Choose an interface(**인터페이스 선택**)**: Active Directory 서버에 연결할 특정 매니지드 디바이스 인터페이스 그룹을 선택합니다.

사용자 동기화 필드

AD Primary Domain(AD 기본 도메인**)**

Microsoft Active Directory 영역에만 해당됩니다. 사용자가 인증해야 하는 Active Directory 서버의 도메인입니다.

참고 모든 Microsoft Active Directory(AD) 영역에 대한 고유 **AD Primary Domain(AD** 기본 도메인**)**을 지정해야 합니다. 다른 Microsoft AD 영역에 동일한 **AD Primary Domain(AD** 기본 도메인**)**을 지정할 수는 있지만, 시스템이 제대로 작동하지 않습니다. 이러한 상황이 발생하는 이유는 시스템이 고유 ID를 각 영역에 있는 모든 사용자에게 할당하기 때문입니다. 따라서 시스템은 특정 사용자 또는 그룹을 확실히 식별할 수 없습니다. 시스템에서 사용자와 그룹을 적절히 식별하지 못하기 때문에 **AD Primary Domain(AD** 기본 도메인**)**이 동일한 영역 하나 이상을 지정할 수 없습니다. 이러한 상황이 발생하는 이유는 시스템이 고유 ID를 각 영역에 있는 모든 사용자에게 할당하기 때문입니다. 따라서 시스템은 특정 사용자 또는 그룹을 확실히 식별할 수 없습니다.

사용자 및 그룹을 찾기 위한 쿼리 입력

Base DN(기본 **DN)**:

(선택 사항) management center이 사용자 데이터 검색을 시작해야 하는 서버의 디렉토리 트리입니다.

일반적으로, 기본 DN(distinguished name)은 회사 도메인 이름 및 운영 단위를 나타내는 기본 구조를 가지고 있습니다. 예를 들어, 예시 회사의 보안 조직은 **`ou=security,dc=example,dc=com`**의 기본 DN을 가질 수 있습니다.

Group DN(그룹 **DN)**:

(선택 사항) management center이 그룹 속성으로 사용자를 검색해야 하는 서버의 디렉토리 트리입니다. 지원되는 그룹 속성 목록은 지원되는 서버 개체 클래스 및 속성 이름, 8 페이지에서 확인할 수 있습니다.

참고 그룹 이름과 조직 단위 이름에는 별표(*), 등호(=), 백슬래시(\) 같은 특수문자가 있으면 안 됩니다. 해당 그룹의 사용자는 다운로드되지 않으며 ID 정책에 사용할 수 없기 때문입니다.

그룹 로드

사용자 인식 및 사용자 제어를 위해 사용자와 그룹을 다운로드할 수 있습니다.

Available Groups(사용 가능한 그룹**), Add to Include(**포함에 추가**), Add to Exclude(**제외에 추가**)**

정책에서 사용할 수 있는 그룹을 제한합니다.

- 그룹을 **Included Groups and Users(**포함된 그룹 및 사용자**)** 또는 **Excluded Groups and Users(**제외된 그룹 및 사용자**)** 필드로 이동하지 않는 한 **Available Groups(**사용 가능한 그룹**)** 필드에 표시되는 그룹은 정책에 사용할 수 있습니다.
- 그룹을 **Included Groups and Users(**포함된 그룹 및 사용자**)** 필드로 이동하면 여기에 포함된 그룹 및 사용자만 다운로드되고 사용자 데이터를 사용자 인식 및 사용자 제어에 사용할 수 있습니다.
- 그룹을 **Excluded Groups and Users(**제외된 그룹 및 사용자**)** 필드로 이동하면 이를 제외하고 여기에 포함된 그룹 및 사용자만 다운로드되고 사용자 인식 및 사용자 제어에 사용할 수 있습니다.
- 포함되지 않은 그룹에 있는 사용자를 포함하려면, 아래 **User Inclusion(**사용자 포함**)** 필드에 사용자 이름을 입력하고 **Add(**추가**)**를 클릭합니다.
- 제외되지 않은 그룹에서 사용자를 제외하려면, 아래 **User Exclusion(**사용자 제외**)** 필드에 사용자 이름을 입력하고 **Add(**추가**)**를 클릭합니다.

참고 management center에 다운로드한 사용자는 **R = I - (E+e) + i** 수식으로 계산하며, 수식의 항목은 다음과 같습니다.

- R은 다운로드한 사용자의 목록입니다.
- I는 포함된 그룹입니다.
- E는 제외된 그룹입니다.
- e는 제외된 사용자입니다.
- i는 포함된 사용자입니다.

지금 동기화

그룹 및 사용자를 AD와 동기화하려면 클릭합니다.

다음 위치에서 자동 동기화 시작

AD에서 사용자 및 그룹을 다운로드할 시간 및 시간 간격을 입력합니다.

Active Directory에 안전하게 연결

Active Directory 서버와 management center(권장 사항)간에 보안 연결을 만들려면 다음 작업을 모두 수행해야 합니다.

- Active Directory 서버의 루트 인증서를 내보냅니다.
- 신뢰할 수 있는 CA 인증서로 루트 인증서를 management center에 가져옵니다.
- Active Directory 서버의 정규화된 이름을 찾습니다.
- 영역 디렉터리를 생성합니다.

자세한 내용은 다음 작업 중 하나를 참조하십시오.

관련 항목

Active Directory 서버의 루트 인증서 내보내기, 31 페이지
Active Directory 서버 이름 찾기, 30 페이지
LDAP 영역 또는 Active Directory 영역 및 영역 디렉터리 생성, 19 페이지

Active Directory 서버 이름 찾기

management center에서 영역 디렉터리를 설정하려면 정규화된 서버 이름을 알아야 합니다. 이 이름은 다음 절차에서 설명하는 대로 찾을 수 있습니다.

시작하기 전에

컴퓨터 이름을 보려면 충분한 권한이 있는 사용자로 Active Directory 서버에 로그인해야 합니다.

프로시저

단계 **1** Active Directory 서버에 로그인합니다.

단계 **2** **Start(**시작**)**를 클릭합니다.

단계 **3** **This PC(**이 **PC)**를 마우스 오른쪽 버튼으로 클릭합니다.

단계 **4** **Properties(**속성**)**를 클릭합니다.

단계 **5** **Advanced System Settings**(고급 시스템 설정)를 클릭합니다.

단계 **6** **Computer Name(**컴퓨터 이름**)** 탭을 클릭합니다.

단계 **7** 전체 컴퓨터 이름의 값을 기록해 둡니다.
FMC에서 영역 디렉터리를 설정할 때 이 이름을 정확하게 입력해야 합니다.

다음에 수행할 작업

LDAP 영역 또는 Active Directory 영역 및 영역 디렉터리 생성, 19 페이지.

관련 항목

Active Directory 서버의 루트 인증서 내보내기, 31 페이지

Active Directory 서버의 루트 인증서 내보내기

다음 작업에서는 Active Directory 서버의 루트 인증서를 내보내는 방법을 설명합니다. 이 인증서는 사용자 ID 정보를 얻기 위해 management center에 안전하게 연결하는 데 필요합니다.

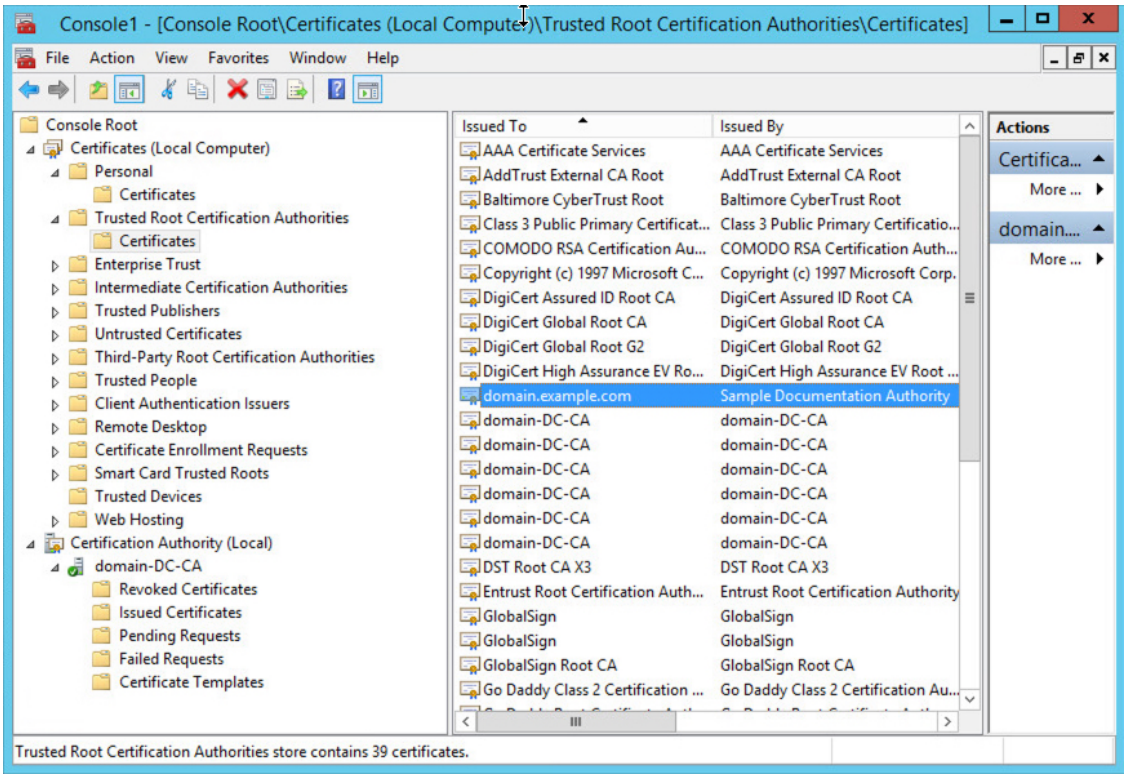
시작하기 전에

Active Directory 서버 루트 인증서의 이름을 알아야 합니다. 루트 인증서의 이름이 도메인과 같거나 인증서의 이름이 다를 수 있습니다. 다음 절차에서는 이름을 찾을 수 있는 한 가지 방법을 보여줍니다. 다른 방법이 있을 수도 있습니다

프로시저

단계 **1** 다음은 Active Directory 서버 루트 인증서의 이름을 찾는 한 가지 방법입니다. 자세한 내용은 Microsoft 설명서를 참조하십시오.

a) Microsoft Management Console을 실행할 권한이 있는 사용자로 Active Directory 서버에 로그인합니다.
b) **Start(**시작**)**를 클릭하고 **mmc**를 입력합니다.
c) **File(**파일**)** > **Add/Remove Snap-in(**스냅인 추가/제거**)**을 클릭합니다.
d) 왼쪽 창의 Available Snap-ins(사용 가능한 스냅인) 목록에서 **Certificates(local)(**인증서**(**로컬**))**을 클릭합니다.
e) **Add(**추가**)**를 클릭합니다.
f) Certificates snap-in(인증서 스냅인) 대화 상자에서 **Computer Account(**컴퓨터 계정**)**를 클릭하고 **Next(**다음**)**를 클릭합니다.
g) Select Computer(컴퓨터 선택) 대화 상자에서 **Local Computer(**로컬 컴퓨터**)**를 클릭하고 **Finish(**마침**)**를 클릭합니다.
h) *Windows Server 2012*만 해당. 인증 기관 스냅인을 추가하려면 위의 단계를 반복합니다.
i) **Console Root(**콘솔 루트**)** > **Trusted Certification Authorities(**신뢰할 수 있는 인증 기관**)** > **Certificates(**인증서**)**를 클릭합니다.
서버의 신뢰할 수 있는 인증서가 오른쪽 창에 표시됩니다. 다음 그림은 Windows Server 2012의 예시일뿐입니다. 사용자마다 다르게 보일 수 있습니다.



단계 **2** **certutil** 명령을 사용하여 인증서를 내보냅니다.

이것이 인증서를 내보내는 유일한 방법입니다. 이 방법은 특히 웹 브라우저를 실행하고 Active Directory 서버에서 management center에 연결할 수 있는 경우 인증서를 내보내는 편리한 방법입니다.

a) **Start(**시작**)**를 클릭하고 **cmd**를 입력합니다.

b) **certutil -ca.cert** *certificate-name* 명령을 입력합니다.
서버의 인증서가 화면에 표시됩니다.

c) 전체 인증서를 클립 보드에 복사합니다. **-----BEGIN CERTIFICATE-----**(으)로 시작하여 **-----END CERTIFICATE-----**(으)로 끝납니다(해당 문자열 포함).

다음에 수행할 작업

신뢰할 수 있는 CA 개체 추가에서 설명한 대로 Active Directory 서버의 인증서를 신뢰할 수 있는 CA 인증서로 management center에 가져옵니다.

관련 항목

Active Directory 서버 이름 찾기, 30 페이지

사용자 및 그룹 동기화

사용자 및 그룹 동기화는 management center가 사용자가 해당 그룹의 그룹 및 사용자에 대해 설정한 영역 및 디렉터리를 쿼리함을 의미합니다. management center에서 찾은 모든 사용자를 ID 정책에서 사용할 수 있습니다.

문제가 발견되면 management center에서 로드할 수 없는 사용자 및 그룹이 포함된 영역을 추가해야 할 가능성이 높습니다. 자세한 내용은 영역 및 신뢰할 수 있는 도메인, 3 페이지를 참조하십시오.

시작하기 전에

각 Active Directory 포리스트에 대한 management center 영역과 각 포리스트의 각 Active Directory 도메인 컨트롤러에 대한 management center 디렉터리를 만듭니다. LDAP 영역 또는 Active Directory 영역 및 영역 디렉터리 생성, 19 페이지을 참조하십시오.

참고 Microsoft Azure AD 영역의 경우 사용자 및 그룹을 동기화할 필요가 없습니다.

사용자 제어에서 사용할 사용자가 있는 도메인에 대해서만 영역을 생성해야 합니다.

Microsoft AD 그룹을 중첩할 수 있으며, Secure Firewall Management Center에서는 해당 그룹과 포함된 사용자를 다운로드합니다. LDAP 영역 또는 Active Directory 영역 및 영역 디렉터리 생성, 19 페이지에 설명된 대로 다운로드할 그룹 및 사용자를 필요에 따라 제한할 수 있습니다.

프로시저

단계 **1** 아직 로그인하지 않았다면 management center에 로그인합니다.

단계 **2** **Integration(통합)** > **Other Integrations(기타 통합)** > **Realms(영역)** 버튼을 클릭합니다.

단계 **3** 각 영역 옆의 **Download(다운로드)** ( )을 클릭합니다.

단계 **4** 결과를 보려면 **Sync Results(결과 동기화)** 탭을 클릭합니다.
Realms(영역) 열은 Active Directory 포리스트에서 사용자 및 그룹을 동기화하는 데 문제가 있는지 여부를 나타냅니다. 각 영역 옆의 다음 표시기를 확인합니다.

영역 열의 표시기	의미
(없음)	모든 사용자 및 그룹이 오류 없이 동기화되었습니다. 조치가 필요하지 않습니다.
노란색 삼각형 ( )	사용자 및 그룹을 동기화하는 동안 문제가 발생했습니다. 각 Active Directory 도메인에 대한 영역과 각 Active Directory 도메인 컨트롤러에 대한 디렉터리를 추가했는지 확인합니다. 자세한 내용은 도메인 간 신뢰 문제 해결, 49 페이지를 참조하십시오.

영역 시퀀스 생성

다음 절차를 수행하면 시스템에서 ID 정책을 적용할 때 검색하는 영역의 순서가 지정된 목록인 영역 시퀀스를 생성할 수 있습니다. 영역을 추가하는 것과 정확히 동일한 방식으로 ID 규칙에 영역 시퀀스를 추가합니다. 차이점은 시스템이 ID 정책을 적용할 때 영역 시퀀스에 지정된 순서대로 모든 영역을 검색한다는 점입니다.

시작하기 전에

각각 Active Directory 서버와의 연결에 해당하는 영역을 2개 이상 생성하고 활성화해야 합니다. LDAP 영역에 대한 영역 시퀀스를 생성할 수 없습니다.

LDAP 영역 또는 Active Directory 영역 및 영역 디렉터리 생성, 19 페이지에 설명된 대로 영역을 생성합니다.

프로시저

단계 **1** 아직 하지 않았다면 management center에 로그인합니다.

단계 **2** **Integration(**통합**)** > **Other Integrations(**기타 통합**)** > **Realms(**영역**)** > **Realm Sequences(**영역 시퀀스**)** 버튼을 클릭합니다.

단계 **3** **Add Sequence(**시퀀스 추가**)**를 클릭합니다.

단계 **4** **Name(**이름**)** 필드에 영역 시퀀스를 식별하는 이름을 입력합니다.

단계 **5** (선택 사항). **Description(**설명**)** 필드에 영역 시퀀스에 대한 설명을 입력합니다.

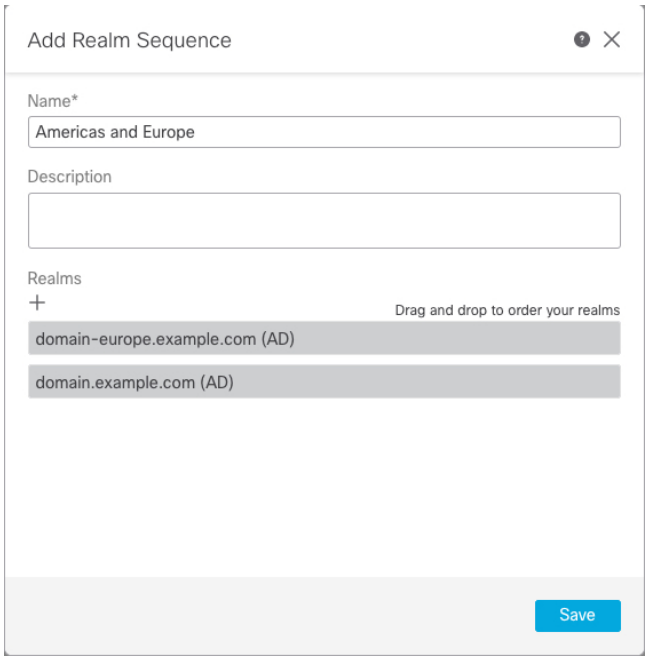
단계 **6** Realms(영역) 아래에서 **Add(**추가**)** (+)를 클릭합니다.

단계 **7** 시퀀스에 추가할 각 영역의 이름을 클릭합니다.

검색 범위를 좁히려면 **Filter(**필터**)** 필드에 영역 이름의 전체 또는 일부를 입력합니다.

단계 **8** **OK(**확인**)**를 클릭합니다.

단계 **9** Add Realm Sequence(영역 시퀀스 추가) 대화 상자에서 시스템이 검색할 순서대로 영역을 끌어다 놓습니다.
다음 그림에는 두 개의 영역으로 구성된 영역 시퀀스의 예가 나와 있습니다. **domain.example.com** 영역보다 먼저 **domain-europe.example.com** 영역을 검색합니다.



단계 **10** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

ID 정책 생성의 내용을 참조하십시오.

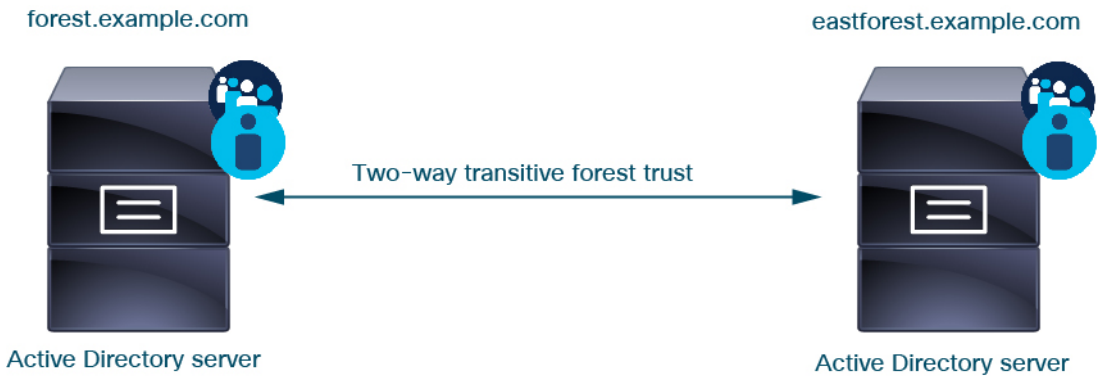
도메인 간 신뢰를 위한 **Management Center** 구성: 설정

이 섹션에서는 도메인 간 신뢰를 사용하는 두 가지 영역으로 management center를 구성하는 과정을 안내하는 여러 항목을 소개합니다.

이 단계별 예시에는 두 개의 포리스트 **forest.example.com** 및 **eastforest.example.com**가 포함되어 있습니다. 포리스트는 각 포리스트의 특정 사용자 및 그룹이 다른 포리스트의 Microsoft AD에 의해 인증될 수 있도록 구성됩니다.

참고 이 항목은 Microsoft AD 영역에만 적용됩니다. Microsoft Azure AD 영역에는 적용되지 않습니다.

다음은 이 예에서 사용된 설정 예입니다.



위의 예를 사용하여 다음과 같이 management center를 설정합니다.

- 액세스 제어 정책으로 제어하려는 사용자가 포함된 **forest.example.com**의 도메인에 대한 영역 및 디렉터리
- 액세스 제어 정책으로 제어하려는 사용자가 포함된 **eastforest.example.com**의 도메인에 대한 영역 및 디렉터리

이 예의 각 영역에는 management center에 디렉터리로 구성된 도메인 컨트롤러가 하나씩 있습니다. 이 예의 디렉터리는 다음과 같이 구성됩니다.

- **forest.example.com**
  - 사용자의 기본 고유 이름(DN): **ou=UsersWest,dc=forest,dc=example,dc=com**
  - 그룹의 기본 DN: **ou=EngineringWest,dc=forest,dc=example,dc=com**
- **eastforest.example.com**
  - 사용자의 기본 DN: **ou=EastUsers,dc=eastforest,dc=example,dc=com**
  - 그룹의 기본 DN: **ou=EastEngineering,dc=eastforest,dc=example,dc=com**

관련 항목

도메인 간 신뢰를 위한 Secure Firewall Management Center 구성 1 단계: 영역 및 디렉터리 구성, 36 페이지

도메인 간 신뢰를 위한 **Secure Firewall Management Center** 구성 **1** 단계: 영역 및 디렉터리 구성

이는 단계별 절차의 첫 번째 작업으로, 엔터프라이즈 조직에서 점점 더 많이 사용되는 구성인 도메인 간 신뢰 관계에 구성된 Active Directory 서버를 인식하도록 management center를 구성하는 방법을 설명합니다. 샘플 구성에 대한 개요는 도메인 간 신뢰를 위한 Management Center 구성: 설정, 35 페이지의 내용을 참고하십시오.

각 도메인에 대해 하나의 영역을 사용하고 각 도메인 컨트롤러에 대해 하나의 디렉토리를 사용하도록 시스템을 설정할 경우, 시스템은 최대 100,000개의 외부 보안 주체(사용자 및 그룹)를 검색할 수 있습니다. 이러한 외부 보안 주체가 다른 영역에서 다운로드한 사용자와 일치하는 경우 액세스 제어 정책에서 사용할 수 있습니다.

시작하기 전에

도메인 간 신뢰 관계에서 Microsoft Active Directory 서버를 구성해야합니다. 자세한 내용은 영역 및 신뢰할 수 있는 도메인, 3 페이지의 내용을 참조하십시오.

LDAP 또는 Microsoft Azure AD로 사용자를 인증하는 경우 이 절차를 사용할 수 없습니다.

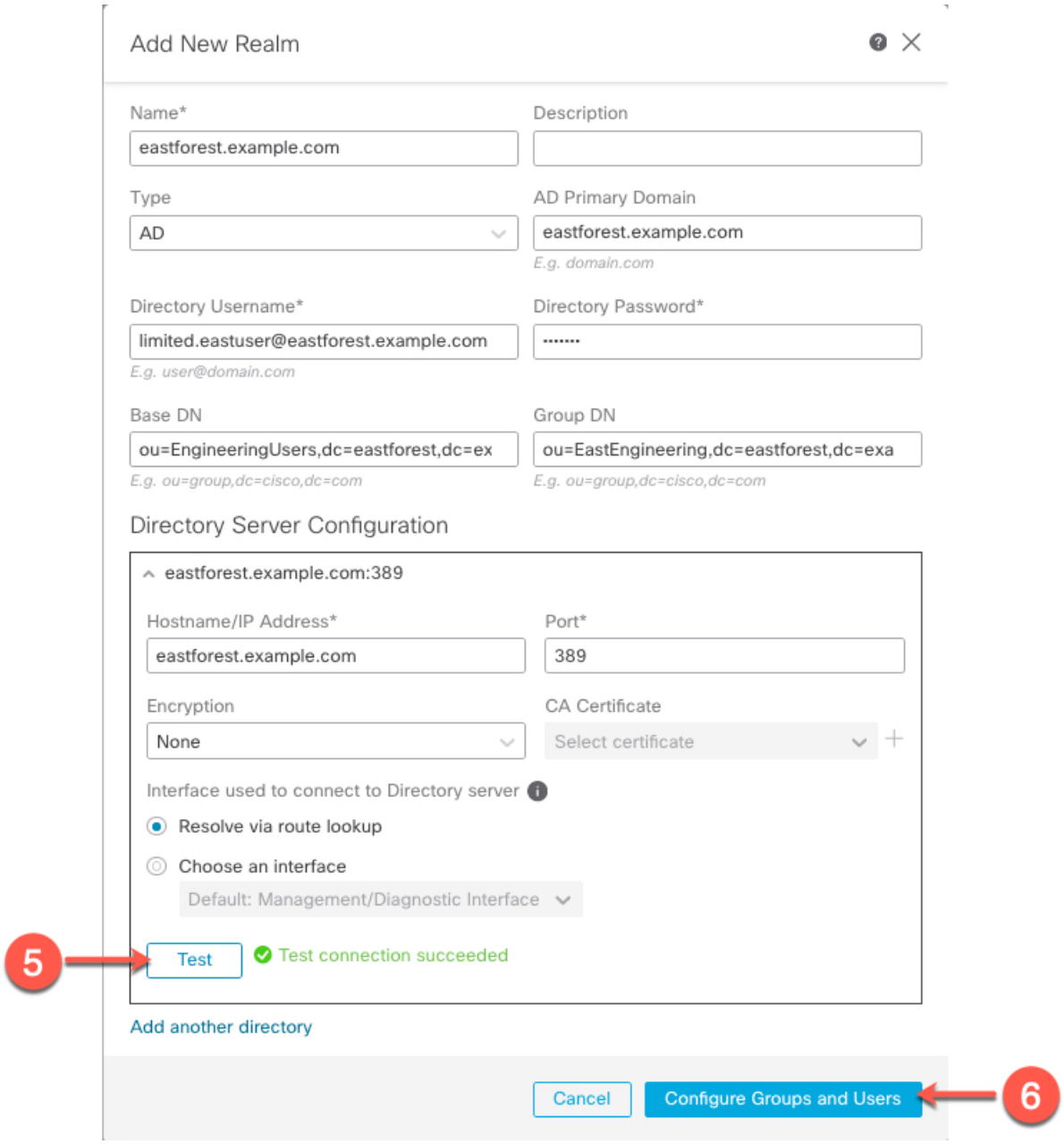
프로시저

단계 **1** management center에 로그인합니다.

단계 **2** **Integration(**통합**)** > **Other Integrations(**기타 통합**)** > **Realms(**영역**)** 버튼을 클릭합니다.

단계 **3** **Add Realm(**영역 추가**)** 드롭다운 목록에서 선택합니다. .

단계 **4** 다음 정보를 입력하여 **forest.example.com**을(를) 구성합니다.



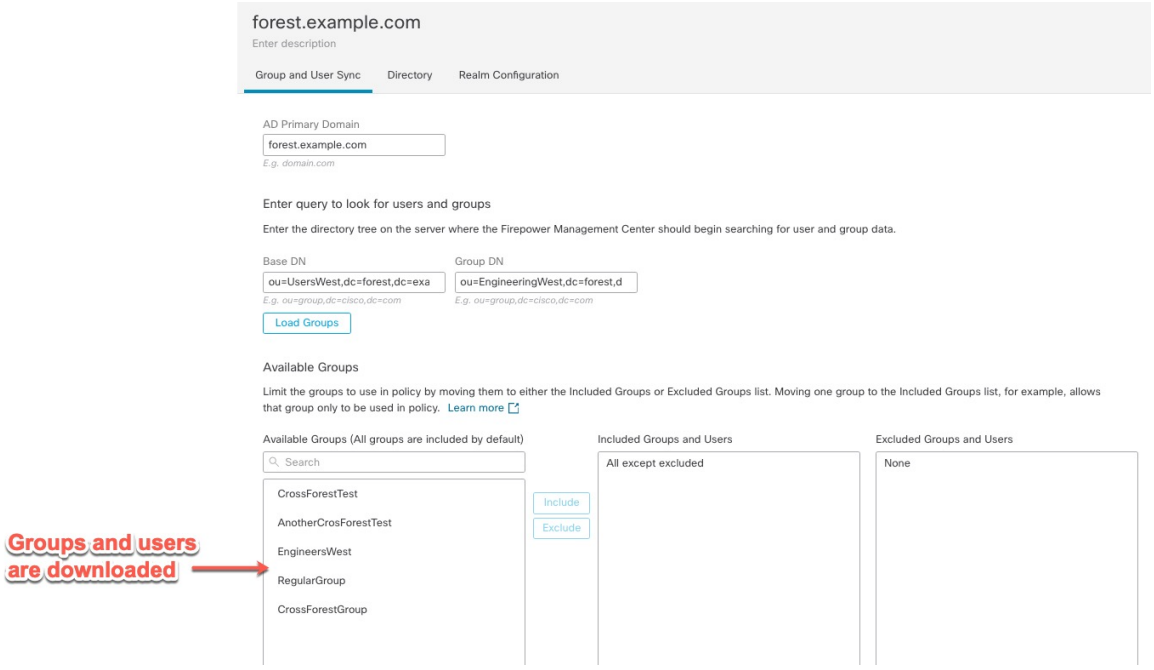
참고 디렉터리 사용자 이름은 Active Directory 도메인의 모든 사용자가 될 수 있습니다. 특별한 권한이 필요하지 않습니다.

디렉터리 서버에 연결하는 데 사용되는 인터페이스는 Active Directory 서버에 연결할 수 있는 모든 인터페이스 일 수 있습니다.

단계 **5** 계속하기 전에 **Test(**테스트**)**를 클릭하고 테스트가 성공했는지 확인합니다.

단계 **6** **Configure Groups and Users(**그룹 및 사용자 설정**)**를 클릭합니다.

단계 **7** 구성에 성공한 경우 다음과 유사한 다음 페이지가 표시됩니다.



참고 그룹 및 사용자가 다운로드되지 않은 경우 **Base DN(**기본 **DN)** 및 **Groups DN(**그룹 **DN)** 필드의 값을 확인하고 **Load Groups(**그룹 로드**)**를 클릭합니다

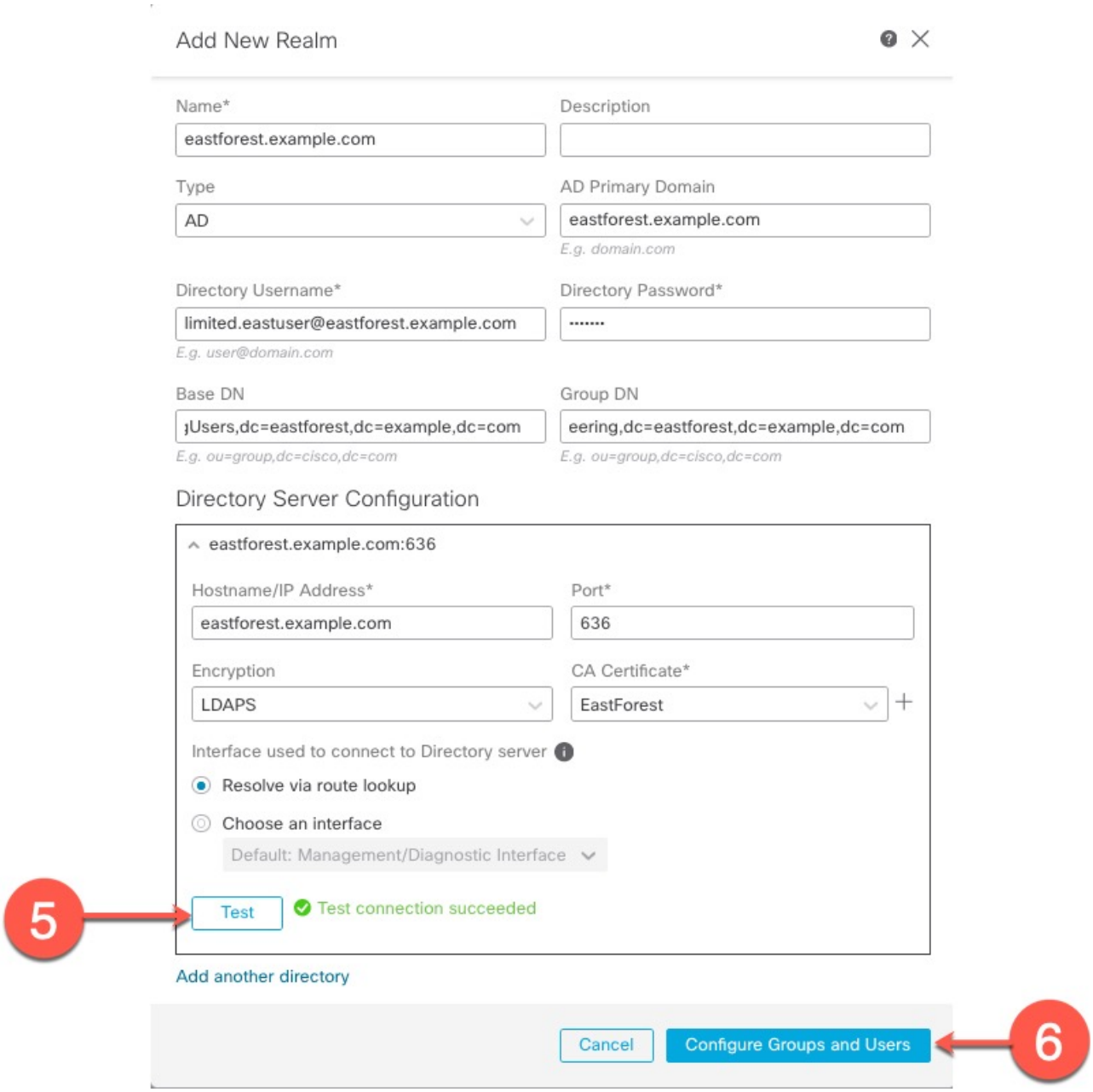
이 페이지에서 사용 가능한 다른 선택적 구성이 있습니다. 자세한 내용은 영역 필드, 23 페이지 및 영역 디렉터리 및 동기화 필드, 27 페이지의 내용을 참조하십시오.

단계 **8** 이 페이지 또는 탭 페이지를 변경한 경우 **Save(**저장**)**를 클릭합니다.

단계 **9** **Integration(**통합**)** > **Other Integrations(**기타 통합**)** > **Realms(**영역**)** 버튼을 클릭합니다.

단계 **10** **Add Realm(**영역 추가**)**을 클릭합니다.

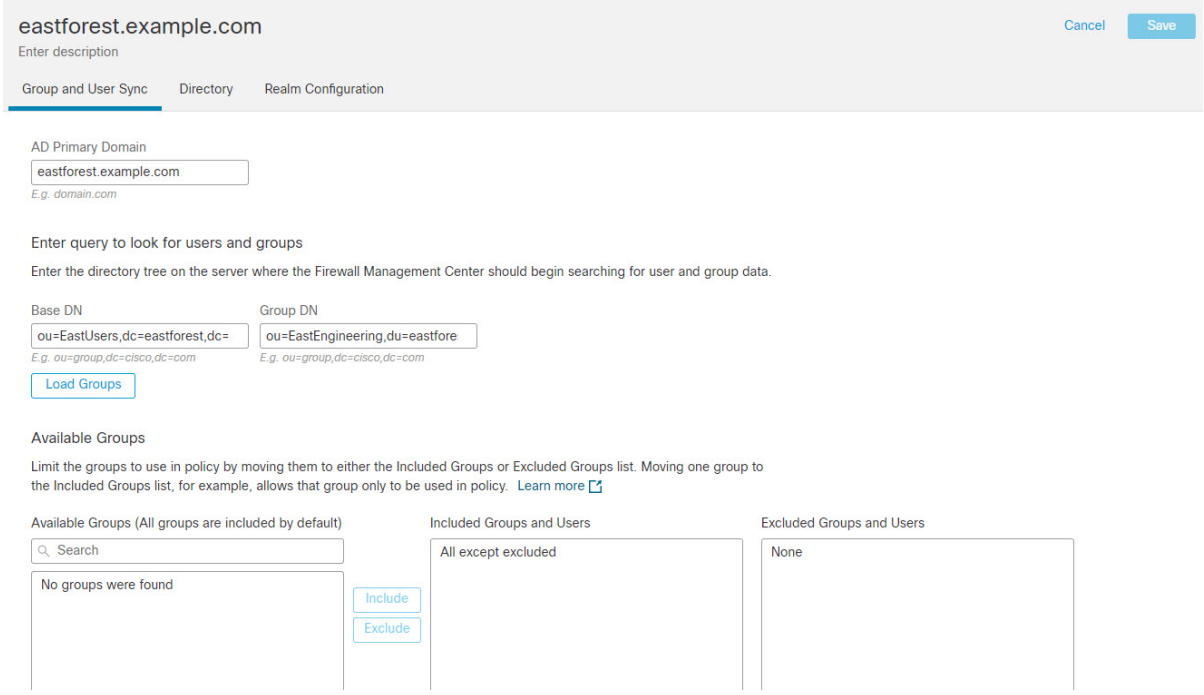
단계 **11** 다음 정보를 입력하여 **eastforest.example.com**을(를) 구성합니다.



단계 **12** 계속하기 전에 **Test(**테스트**)**를 클릭하고 테스트가 성공했는지 확인합니다.

단계 **13** **Configure Groups and Users(**그룹 및 사용자 설정**)**를 클릭합니다.

단계 **14** 구성에 성공한 경우 다음과 유사한 다음 페이지가 표시됩니다.



관련 항목

도메인 간 신뢰를 위한 management center 구성 2단계: 사용자 및 그룹 동기화, 41 페이지

도메인 간 신뢰를 위한 **management center** 구성 **2**단계: 사용자 및 그룹 동기화

도메인 간 신뢰 관계가 있는 둘 이상의 Active Directory 서버를 구성한 후에는 사용자 및 그룹을 다운로드해야 합니다. 이 프로세스를 수행하면 Active Directory 구성에 발생할 수있는 문제(예: 그룹 또는 사용자가 한 Active Directory 도메인에 대해 다운로드되었지만 다른 Active Directory 도메인에 대해서는 다운로드되지 않음)가 표시됩니다.

시작하기 전에

도메인 간 신뢰를 위한 Secure Firewall Management Center 구성 1 단계: 영역 및 디렉터리 구성, 36 페이지에서 설명한 작업을 수행했는지 확인합니다.

프로시저

단계 **1** management center에 로그인합니다.

단계 **2** **Integration(**통합**)** > **Other Integrations(**기타 통합**)** > **Realms(**영역**)** 버튼을 클릭합니다.

단계 **3** 도메인 간 신뢰의 영역 행 끝에서 (지금 다운로드)를 클릭 한 다음 **Yes(**예**)**를 클릭합니다.

단계 **4** **Check Mark(**확인 표시**)** () (알림) > **Tasks(**작업**)**를 클릭합니다.

그룹 및 사용자를 다운로드하지 못하면 다시 시도하십시오. 후속 시도가 실패할 경우 영역 필드, 23 페이지및 영역 디렉터리 및 동기화 필드, 27 페이지에 설명된 대로 영역 및 디렉터리 설정을 검토합니다.

단계 **5** **Integration(**통합**)** > **Other Integrations(**기타 통합**)** > **Realms(**영역**)** > **Sync Results(**동기화 결과**)** 버튼을 클릭합니다.

관련 항목

도메인 간 신뢰를 위한 management center 구성 3단계: 문제 해결, 42 페이지

도메인 간 신뢰를 위한 **management center** 구성 **3**단계: 문제 해결

management center에서 도메인 간 신뢰를 설정하는 마지막 단계는 사용자 및 그룹을 오류없이 다운로드하는 것입니다. 사용자 및 그룹이 제대로 다운로드되지 않는 일반적인 이유는 해당 사용자가 속한 영역이 management center에 다운로드되지 않았기 때문입니다.

이 항목에서는 도메인 컨트롤러 계층 구조에서 그룹을 찾도록 영역이 구성되지 않았으므로 한 포리스트에서 참조되는 그룹을 다운로드할 수 없음을 진단하는 방법에 대해 설명합니다.

시작하기 전에

프로시저

단계 **1** 아직 하지 않았다면 management center에 로그인합니다.

단계 **2** **Integration(**통합**)** > **Other Integrations(**기타 통합**)** > **Realms(**영역**)** > **Sync Results(**동기화 결과**)** 버튼을 클릭합니다.

Realm(영역) 열에서 영역 이름 옆에 노란색 삼각형 ()가 표시되어 있으면 해결해야 하는 문제가있는 것입니다. 그렇지 않은 경우 결과가 올바르게 구성되어 종료할 수 있습니다.

단계 **3** 문제가 표시되는 영역에서 사용자 및 그룹을 다시 다운로드합니다.

a) **Realms(**영역**)** 탭을 클릭합니다.

b)  (Download Now (지금 다운로드))를 클릭한 다음 **Yes(**예**)**를 클릭합니다.

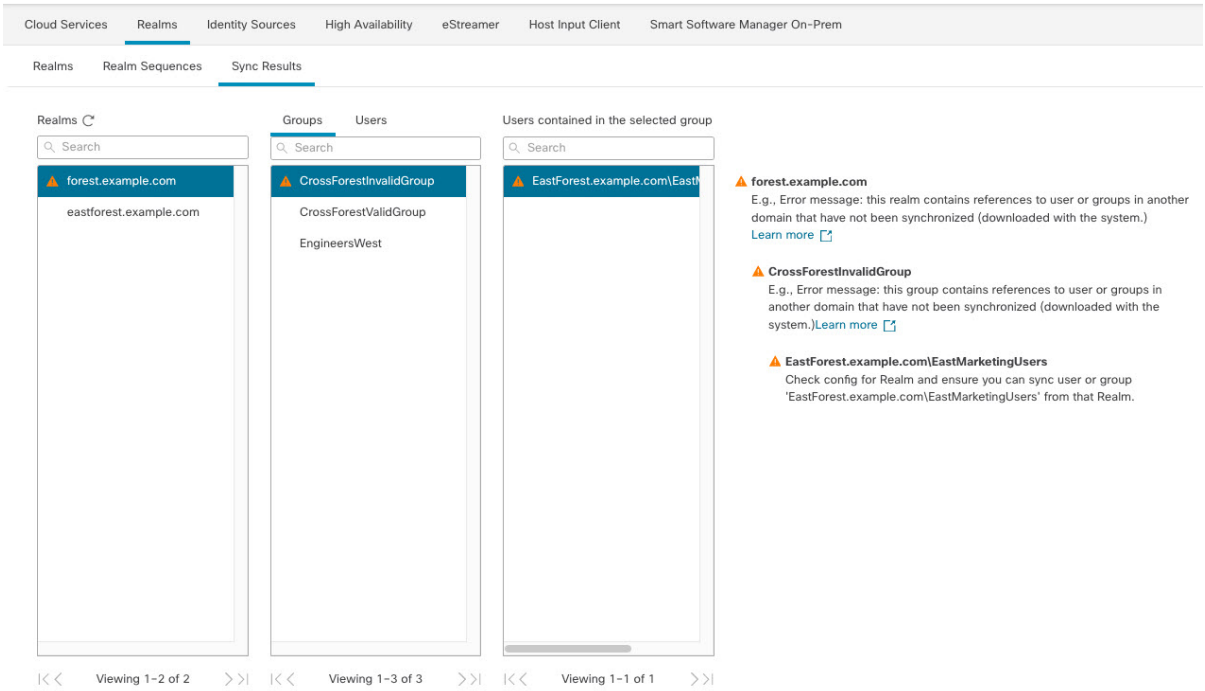
단계 **4** **Sync Results(**결과 동기화**)** 탭 페이지를 클릭합니다.

노란색 삼각형 ()이 Realms(영역) 열에 표시되면 문제가있는 영역 옆의 노란색 삼각형 ()을 클릭합니다.

단계 **5** 가운데 열에서 **Groups(**그룹**)** 또는 **Users(**사용자**)**를 클릭하여 자세한 정보를 찾습니다.

단계 **6** Groups or Users(그룹 또는 사용자) 탭 페이지에서 노란색 삼각형 ()을 클릭하여 추가 정보를 표시합니다.

오른쪽 열에는 문제의 원인을 격리할 수 있는 충분한 정보가 표시되어야 합니다.



위의 예에서는 **forest.example.com**에 management center에서 다운로드하지 않은 다른 그룹 **CrossForestInvalidGroup** 을 포함하는 크로스 도메인 그룹 **EastMarketingUsers**을 포함합니다 **eastforest.example.com** 영역을 다시 동기화한 후에도 오류가 해결되지 않으면 Active Directory 도메인 컨트롤러가 **EastMarketingUsers**을 포함하지 않았음을 의미합니다.

이 문제를 해결하려면, 다음을 수행합니다.

- **CrossForestInvalidGroup**에서 **EastMarketingUsers**를 제거하고 **forest.example.com** 영역을 다시 동기화한 후 다시 확인합니다.
- **eastforest.example.com** 영역의 그룹 **DN**에서 **ou=EastEngineering** 값을 제거합니다. 그러면 management center가 Active Directory 계층 구조의 최상위 레벨에서 그룹을 검색하고 **eastforest.example.com**을 동기화한 후 다시 확인합니다.

영역 관리

이 섹션에서는 Realms(영역) 페이지에서 컨트롤을 사용해 영역에 대한 유지 관리 작업을 수행하는 방법을 설명합니다. 다음에 유의하십시오.

- 컨트롤이 흐리게 표시되는 경우에는 컨피그레이션이 상위 도메인에 속하거나 컨피그레이션을 수정할 권한이 없는 것입니다.
- **View(보기)** ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

프로시저

단계 **1** 아직 하지 않았다면 management center에 로그인합니다.

단계 **2** **Integration(**통합**)** > **Other Integrations(**기타 통합**)** > **Realms(**영역**)** 버튼을 클릭합니다.

단계 **3** 영역을 삭제하려면 **Delete(**삭제**)** ( )을 클릭합니다.

단계 **4** 영역을 편집하려면 영역 옆의 **Edit(**수정**)** ( )을 클릭하고 LDAP 영역 또는 Active Directory 영역 및 영역 디렉터리 생성, 19 페이지에 설명된 대로 영역을 변경합니다.

단계 **5** 영역을 활성화하려면 **State(**상태**)**를 오른쪽으로 밉니다. 영역을 비활성화하려면 왼쪽으로 밉니다.

단계 **6** 사용자 및 사용자 그룹을 다운로드하려면 **Download(**다운로드**)** ( )을 클릭합니다.

단계 **7** 영역을 복사하려면 **Copy(**복사**)** ( )을 클릭합니다.

단계 **8** 영역을 비교하려면 영역 비교, 44 페이지를 참고하십시오.

영역 비교

이 작업을 수행하려면 관리자, 액세스 관리자, 네트워크 관리자 또는 보안 승인자이어야 합니다.

프로시저

단계 **1** management center에 로그인합니다.

단계 **2** **Integration(**통합**)** > **Other Integrations(**기타 통합**)** > **Realms(**영역**)** 버튼을 클릭합니다.

단계 **3** **Compare Realms(**영역 비교**)**를 클릭합니다.

단계 **4** **Compare Against(**비교 대상**)** 목록에서 **Compare Realm(**영역 비교**)**을 선택합니다.

단계 **5** **Realm A(**영역 **A)** 및 **Realm B(**영역 **B)** 목록에서 비교할 영역을 선택합니다.

단계 **6** **OK(**확인**)**를 클릭합니다.

단계 **7** 변경 사항을 개별적으로 탐색하려면 제목 표시줄 위의 **Previous(**이전**)** 또는 **Next(**다음**)**를 클릭합니다.

단계 **8** (선택 사항). **Comparison Report(**비교 보고서**)**를 클릭하여 영역 비교 보고서를 생성합니다.

단계 **9** (선택 사항). **New Comparison(**새 비교**)**을 클릭하여 새 영역 비교 보기를 생성합니다.

영역 및 사용자 다운로드 문제 해결

서버 연결 동작이 정상적이지 않을 경우 영역 컨피그레이션, 디바이스 설정 또는 서버 설정을 조정하는 방법을 고려하십시오. 기타 관련 문제 해결 정보를 보려면 다음을 참조하십시오.

- ISE/ISE-PIC 또는 Cisco TrustSec 문제 해결

- TS 에이전트 ID 소스 문제 해결
- 캡티브 포털(captive portal) ID 소스 문제 해결
- 원격 액세스 VPN ID 소스 문제 해결
- 사용자 제어 문제 해결

증상: 영역 및 그룹이 보고되었지만 다운로드되지는 않음

management center의 상태 모니터는 사용자 또는 영역의 불일치를 알려주며, 이러한 불일치는 다음과 같이 정의됩니다.

- 사용자 불일치: 사용자가 다운로드되지 않고 management center에 보고됩니다.

  사용자 불일치가 발생하는 일반적인 이유는 사용자가 management center 다운로드에서 제외된 그룹에 속하기 때문입니다. Cisco Secure Firewall Management Center 디바이스 구성 가이드에서 논의된 정보를 검토합니다.

- 영역 불일치: 사용자가 management center의 알 수 없는 영역에 해당하는 도메인에 로그인합니다.

예를 들어 management center의 **domain.example.com**이라는 도메인에 대응하는 영역을 정의했지만 로그인이 **another-domain.example.com**이라는 도메인에서 보고되었다면, 이것은 영역 불일치가 됩니다. 이 도메인의 사용자는 management center가 Unknown(알 수 없음)으로 식별합니다.

불일치 임계값이 백분율로 설정되며, 해당 값보다 높으면 상태 경고가 트리거됩니다. 예:

- 기본 불일치 임계값 50%를 사용하고 여덟 개 수신 세션에서 두 개 영역이 불일치하는 경우, 불일치 비율은 25%이고 어떠한 경고도 트리거되지 않습니다.
- 불일치 임계값을 30%로 설정하고 다섯 개 수신 세션에서 세 개 영역이 불일치하는 경우, 불일치 비율은 60%이며 경고가 트리거됩니다.

ID 규칙과 일치하지 않는 Unknown users(알 수 없는 사용자)에게 적용되는 정책은 없습니다. (Unknown users(알 수 없는 사용자)에 ID 규칙을 설정할 수 있지만, 사용자와 영역을 정확하게 식별하여 규칙 수를 최소한으로 유지하는 것이 좋습니다.)

자세한 내용은 영역 또는 사용자 불일치 탐지, 48 페이지를 참고하십시오.

증상: 사용자가 다운로드되지 않음

가능한 원인은 다음과 같습니다.

- 영역 **Type(유형)**을 잘못 설정한 경우, 사용자와 그룹을 다운로드할 수 없습니다. 시스템이 기대하는 속성과 저장소가 제공하는 속성이 일치하지 않기 때문입니다. 예를 들어 Microsoft Active Directory 영역의 **Type(유형)**을 **LDAP**로 설정하면, 시스템은 Active Directory에서 `none(없음)`으로 설정되는 `uid` 속성을 기대합니다. (Active Directory 저장소는 사용자 ID에 `sAMAccountName`을 사용합니다.)

  솔루션: 영역 **Type(유형)** 필드를 적절하게 설정합니다. Microsoft Active Directory의 경우에는 **AD**이며, 다른 지원되는 LDAP 저장소의 경우에는 **LDAP**입니다.

- 그룹 또는 조직 단위 이름에 특수 문자가 있는 Active Directory 그룹의 사용자는 ID 정책 규칙에 사용하지 못할 수도 있습니다. 예를 들어 그룹 또는 조직 단위 이름에 별표(*), 등호(=), 백슬래시(\) 같은 특수문자가 있다면, 해당 그룹의 사용자는 다운로드되지 않으며 ID 정책에 사용할 수 없습니다.

  솔루션: 그룹 또는 조직 단위 이름에서 특수 문자를 제거합니다.

중요 Secure Firewall Management Center와 Active Directory 도메인 컨트롤러 간의 레이턴시를 줄이려면 Secure Firewall Management Center와 최대한 지리적으로 가까운 영역 디렉터리(즉, 도메인 컨트롤러)를 구성하는 것이 좋습니다.

예를 들어 Secure Firewall Management Center가 북미에 있는 경우 북미에도 있는 영역 디렉터리를 구성합니다. 그렇지 않으면 사용자 및 그룹 다운로드 시간 초과 등의 문제가 발생할 수 있습니다.

증상: 영역의 모든 사용자가 다운로드되지 않음

가능한 원인은 다음과 같습니다.

- 한 영역에서 최대 사용자 수를 초과하여 다운로드하려고 하면 최대 사용자 수에서 다운로드가 중지되고 상태 알림이 표시됩니다. 사용자 다운로드 제한은 Secure Firewall Management Center 모델별로 설정됩니다. 자세한 내용은 Microsoft Active Directory에 대한 사용자 제한을 참조하십시오.
- 모든 사용자는 그룹의 구성원이어야 합니다. 그룹의 구성원이 아닌 사용자는 다운로드되지 않습니다.

증상: 액세스 제어 정책이 그룹 구성원 자격과 일치하지 않음

이 솔루션은 다른 AD 도메인과 트러스트 관계에 있는 AD 도메인에 적용됩니다. 아래 설명 내용에서 외부 도메인이란 사용자가 로그인하는 것과 다른 도메인을 의미합니다.

사용자가 신뢰할 수 있는 외부 도메인의 정의된 그룹에 속하는 경우, management center는 외부 도메인의 구성원 자격을 추적하지 않습니다. 예를 들어 다음과 같은 시나리오를 가정해 보십시오.

- 도메인 컨트롤러 1 및 2는 서로 신뢰합니다.
- 도메인 컨트롤러 2에 그룹 A가 정의되어 있습니다.
- 컨트롤러 1의 사용자 `mparvinder`는 그룹 A의 구성원입니다.

사용자 `mparvinder`가 그룹 A에 있지만, 구성원 자격 그룹 A를 지정하는 management center 액세스 제어 정책 규칙이 일치하지 않습니다.

솔루션: 도메인 컨트롤러 1에 유사한 그룹을 생성합니다. 여기에는 그룹 A에 속한 모든 도메인 1 어카운트가 포함됩니다. 그룹 A 또는 그룹 B의 모든 구성원과 일치하도록 액세스 컨트롤 정책을 변경합니다.

증상: 액세스 제어 정책이 하위 도메인 구성원 자격과 일치하지 않음

사용자가 상위 도메인의 하위 도메인에 속한 경우, Firepower는 도메인 간의 상위/하위 관계를 추적하지 않습니다. 예를 들어 다음과 같은 시나리오를 가정해 보십시오.

- 도메인 `child.parent.com`은 `parent.com`의 하위 도메인입니다.
- 사용자 `mparvinder`는 `child.parent.com`에 정의되어 있습니다.

사용자 `mparvinder`가 하위 도메인에 있더라도, `parent.com`과 일치하는 Firepower 액세스 컨트롤 정책은 `child.parent.com` 도메인의 `mparvinder`와 일치하지 않습니다.

솔루션: `parent.com` 또는 `child.parent.com`의 구성원 자격과 일치하도록 액세스 제어 정책 규칙을 변경합니다.

증상: 영역 또는 영역 디렉토리 테스트 실패

디렉터리 페이지 (테스트) 버튼 호스트 이름 또는 IP 주소를 입력 한 LDAP 쿼리를 보냅니다. 작업이 실패한다면 다음 사항을 확인해 주십시오.

- 입력한 **Hostname(**호스트 이름**)**은 LDAP 서버 또는 Active Directory 도메인 컨트롤러의 IP 주소로 확인됩니다.
- 입력한 **IP Address(IP** 주소**)**가 유효합니다.

영역 설정 페이지에서 **Test AD Join(AD** 죠인 테스트**)** 버튼을 누르면 다음 사항을 확인합니다.

- DNS는 **AD Primary Domain(AD** 기본 도메인**)**을 LDAP 서버 또는 Active Directory 도메인 컨트롤러의 IP 주소로 확인합니다.
- **AD Join Username(AD** 죠인 사용자 이름**)**과 **AD Join Password(AD** 죠인 비밀번호**)**가 올바릅니다.

  AD Join Username(AD 죠인 사용자 이름**)**은 온전한 이름이어야 합니다(예: **`administrator`**가 아닌 **`administrator@mydomain.com`**).
- 사용자는 도메인에서 컴퓨터를 생성하고 management center를 도메인에 도메인 컴퓨터로 죠인할 권한을 가집니다.

증상: 예기치 않은 시간에 사용자 시간 초과가 발생함

예기치 않은 간격으로 사용자 시간 초과가 발생할 경우 ISE/ISE-PIC 서버의 시간이 Secure Firewall Management Center의 시간과 동기화되었는지 확인하십시오. 어플라이언스가 동기화되지 않은 경우, 시스템이 예기치 않은 간격으로 사용자 시간 초과를 수행할 수 있습니다.

예기치 않은 간격으로 사용자 시간 초과가 발생할 경우 ISE/ISE-PIC 또는 TS 에이전트 서버의 시간이 Secure Firewall Management Center의 시간과 동기화되었는지 확인하십시오. 어플라이언스가 동기화되지 않은 경우, 시스템이 예기치 않은 간격으로 사용자 시간 초과를 수행할 수 있습니다.

증상: 이전에 확인되지 않은 **ISE/ISE-PIC** 사용자에 대한 사용자 데이터가 웹 인터페이스에 표시되지 않음

데이터베이스에 데이터가 아직 없는 ISE/ISE-PIC 또는 TS 에이전트 사용자의 활동이 탐지되면 시스템은 서버에서 관련된 정보를 검색합니다. Microsoft Windows 서버에서 이러한 정보를 정상적으로 검색하기까지 추가 시간이 필요한 경우도 있습니다. 데이터 검색에 성공할 때까지 ISE/ISE-PIC 또는 TS 에이전트 사용자에 의해 확인된 활동이 웹 인터페이스에 표시되지 않습니다.

그리고 이로 인해 시스템이 액세스 제어 규칙을 사용하는 사용자의 트래픽을 처리하지 못할 수도 있습니다.

증상: 이벤트에 예기치 않은 사용자 데이터가 있음

사용자 또는 사용자 활동 이벤트에 예기치 않은 IP 주소가 있을 경우 영역을 확인하십시오. 시스템에서는 동일한 **AD Primary Domain(AD** 기본 도메인**)** 값으로 여러 영역을 구성하는 것을 지원하지 않습니다.

증상: 터미널 서버 로그인에서 비롯된 사용자가 시스템에서 고유하게 식별되지 않음

구축에 터미널 서버가 포함되어 있고 터미널 서버에 연결된 하나 이상의 서버에 대해 영역을 구성한 경우, Cisco TS(Terminal Services) 에이전트를 구축하여 터미널 서버 환경에서 사용자 로그인을 정확하게 보고해야 합니다. TS 에이전트를 설치 및 구성하면 개별 사용자에게 고유 포트가 할당되므로, 시스템이 웹 인터페이스에서 해당 사용자를 고유하게 식별할 수 있습니다.

TS 에이전트에 대한 자세한 내용은 *Cisco TS(Terminal Services)* 에이전트 가이드를 참조하십시오.

영역 또는 사용자 불일치 탐지

이 섹션은 다음과 같이 정의되는 영역 또는 사용자 불일치를 탐지하는 방법을 설명합니다.

- 사용자 불일치: 사용자가 다운로드되지 않고 management center에 보고됩니다.

  사용자 불일치가 발생하는 일반적인 이유는 사용자가 management center 다운로드에서 제외된 그룹에 속하기 때문입니다. Cisco Secure Firewall Management Center 디바이스 구성 가이드에서 논의된 정보를 검토합니다.

- 영역 불일치: 사용자가 management center의 알 수 없는 영역에 해당하는 도메인에 로그인합니다.

자세한 정보는 영역 및 사용자 다운로드 문제 해결, 44 페이지 섹션을 참조하십시오.

ID 규칙과 일치하지 않는 Unknown users(알 수 없는 사용자)에게 적용되는 정책은 없습니다. (Unknown users(알 수 없는 사용자)에 ID 규칙을 설정할 수 있지만, 사용자와 영역을 정확하게 식별하여 규칙 수를 최소한으로 유지하는 것이 좋습니다.)

프로시저

단계 **1** 영역 또는 사용자 불일치 탐지 활성화:

a) 아직 하지 않았다면 management center에 로그인합니다.

b) **System(**시스템**)** > **Health(**상태**)** > **Policy(**정책**)**를 클릭합니다.
c) 새 상태 정책을 만들거나 기존 정책을 편집합니다.
d) Editing Policy(정책 편집) 페이지에서 **Policy Runtime Interval(**정책 런타임 간격**)**을 설정합니다. 이것은 모든 상태 모니터링 작업을 실행하는 빈도가 됩니다.
e) 왼쪽 창에서 **Realm(**영역**)**을 클릭합니다.
f) 다음 정보를 입력합니다.

- **Enabled(**활성화됨**)**: **On(**켜기**)** 클릭
- **Warning Users match threshold(**사용자 경고 일치 임계값**) %**: 상태 모니터에서 경고가 표시되게 하는 영역 불일치 또는 사용자 불일치의 비율입니다. 자세한 내용은 영역 및 사용자 다운로드 문제 해결, 44 페이지를 참고하십시오.

g) 페이지 하단의 **Save Policy & Exit(**정책 저장 및 종료**)**를 클릭합니다.
h) Cisco Secure Firewall Management Center 관리 가이드의 상태 정책 적용에 설명된 대로 상태 정책을 매니지드 디바이스에 적용합니다.

단계 **2** 다음 방법 중 하나를 이용해 사용자 및 영역 불일치를 확인합니다.

- 경고 임계값을 초과한 경우, management center 상단 탐색 창에서 **Warning(**경고**)** > **Health(**상태**)**를 클릭합니다. Health Monitor(상태 모니터)가 열립니다.
- **System(**시스템**)** > **Health(**상태**)** > **Monitor(**모니터**)**를 클릭합니다.

단계 **3** Display(표시) 열의 Health Monitor(상태 모니터링) 페이지에서 **Realm: Domain(**영역**:** 도메인**)** 또는 **Realm: User(**영역**:** 사용자**)**를 확장해 불일치 관련 정보를 확인합니다.

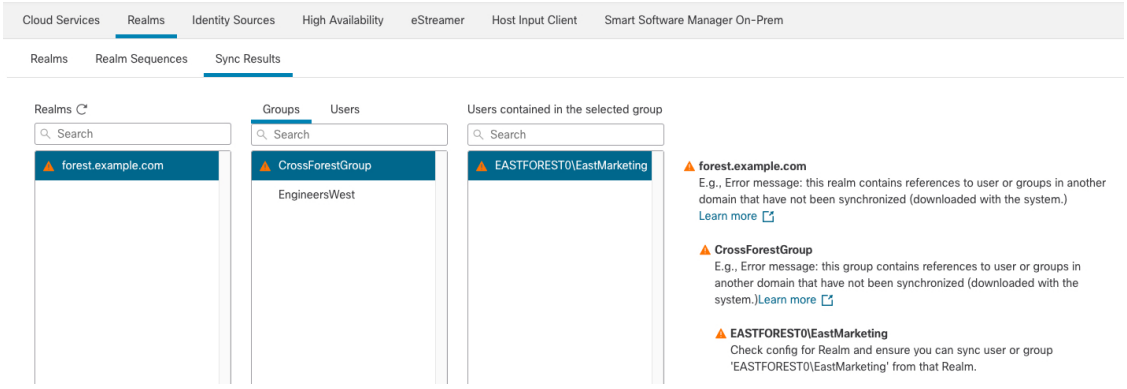
도메인 간 신뢰 문제 해결

도메인 간 신뢰를 위한 management center 설정 문제 해결 시 발생하는 일반적인 문제는 다음과 같습니다.

- 공유 그룹이 있는 모든 포리스트에 대해 영역 또는 디렉터리를 추가하지 않습니다.
- 사용자를 다운로드에서 제외하도록 영역을 설정하면 해당 사용자는 다른 영역의 그룹에서 참조됩니다.
- 특정한 일시적인 문제가 발생합니다.

문제 이해

management center에서 사용자 및 그룹을 Active Directory 포리스트와 동기화하는 데 문제가 있는 경우, Sync Results(동기화 결과) 탭 페이지가 다음과 유사하게 표시됩니다.



다음 테이블에서는 정보를 해석하는 방법을 설명합니다.

열	의미
영역	시스템에 설정된 모든 영역을 표시합니다. 영역 목록을 업데이트하려면 **Refresh(**새로 고침**)**( )을(를) 클릭합니다. 노란색 삼각형 ( ) 영역 문제를 나타내기 위해 표시됩니다. 모든 사용자와 그룹이 성공적으로 동기화된 경우, 영역 옆에 아무것도 표시되지 않습니다.
그룹	영역의 모든 그룹을 표시하려면 **Groups(**그룹**)**를 클릭합니다. 영역과 마찬가지로는 노란색 삼각형 ( )이(가) 문제를 나타내기 위해 표시됩니다. 문제에 대한 자세한 내용을 보려면 노란색 삼각형 ( )을(를) 클릭합니다.
사용자	모든 사용자를 그룹별로 정렬해서 표시하려면 **Users(**사용자**)**를 클릭합니다.
선택한 그룹에 포함된 사용자	Groups(그룹) 열에서 선택한 그룹의 모든 사용자를 표시합니다. 노란색 삼각형 ( )을(를) 클릭하면 테이블 오른쪽에 추가 정보가 표시됩니다.
선택한 사용자를 포함하는 그룹	선택한 사용자가 속한 모든 그룹을 표시합니다. 노란색 삼각형 ( )을 클릭하면 테이블 오른쪽에 추가 정보가 표시됩니다.

열	의미
오류 세부 정보(테이블 오른쪽에 표시)	시스템은 동기화할 수 없는 NetBIOS 포리스트 이름 및 그룹 이름을 표시합니다. 시스템에서 이러한 사용자 및 그룹을 동기화할 수 없는 일반적인 이유는 다음과 같습니다. • 문제: 그룹 및 사용자를 포함하는 포리스트의 management center에 해당 영역이 설정되지 않았습니다. 해결 방법: LDAP 영역 또는 Active Directory 영역 및 영역 디렉터리 생성, 19 페이지에 설명된 대로 그룹을 포함하는 포리스트의 영역을 추가합니다. • 문제: 그룹이 management center로 다운로드되지 않도록 제외했습니다. 해결 방법: **Realms(**영역**)** 탭 페이지를 클릭하고 **Edit(**수정**)** ( )을(를) 클릭한 다음 **Excluded Groups and Users(**제외된 그룹 및 사용자**)** 목록에서 표시된 그룹 또는 사용자를 이동합니다.

사용자 및 그룹을 다시 다운로드해 봅니다.

일시적인 문제일 가능성이 있는 경우, 모든 영역에 대해 사용자 및 그룹을 다운로드합니다.

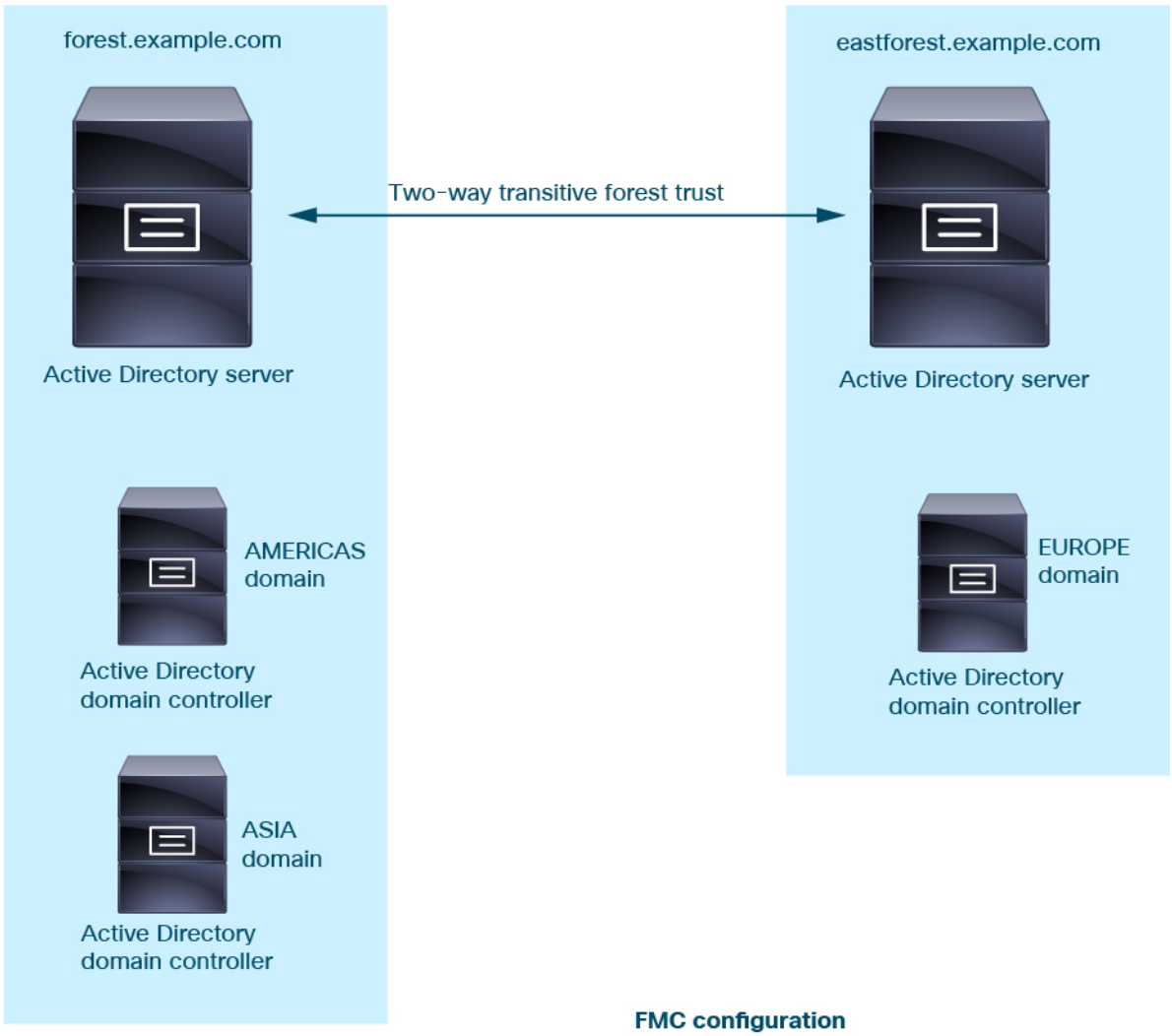
1. 아직 로그인하지 않았다면 management center에 로그인합니다.
2. **Integration(**통합**)** > **Other Integrations(**기타 통합**)** > **Realms(**영역**)** 버튼을 클릭합니다.
3. **Download(**다운로드**)** ( ) 버튼을 클릭합니다.
4. **Sync Results(**결과 동기화**)** 탭 페이지를 클릭합니다.
5. Realms(영역) 열의 항목에 대해 표시기가 표시되지 않으면 문제가 해결된 것입니다.

모든 포리스트에 대한 영역 추가

다음을 설정했는지 확인합니다.

- ID 정책에 사용할 사용자가 있는 각 포리스트의 management center 영역
- ID 정책에 사용할 사용자가 있는 해당 포리스트의 각 도메인 컨트롤러에 대한 management center 디렉터리

다음 그림은 예를 보여줍니다.


forest.example.com
Active Directory server
Two-way transitive forest trust
eastforest.example.com
Active Directory server
AMERICAS
domain
Active Directory
domain controller
EUROPE
domain
Active Directory
domain controller
ASIA
domain
Active Directory
domain controller
FMC configuration
FMC
Realm: forest.example.com
Directory: AMERICAS.forest.example.com
Directory: ASIA.forest.example.com
Realm: eastforest.example.com
Directory: EUROPE.eastforest.example.com

영역 히스토리

기능	최소 **Management Center**	최소 **Threat Defense**	세부 사항
Microsoft Azure AD(Active Directory) 영역.	7.4.0	7.4.0	ISE와 함께 Microsoft Azure AD(Active Directory) 영역을 사용하여 사용자를 인증하고 사용자 제어를 위한 사용자 세션을 가져올 수 있습니다. 신규/수정된 화면: 시스템 (⚙) > **Integration(**통합**)** > **Realms(**영역**)** > **Add Realm(**영역 추가**)** > **Azure AD**
Active Directory 도메인에 대한 도메인 간 신뢰.	7.2.0	7.0.0	서로를 신뢰하는 Microsoft Active Directory (AD) 도메인은 일반적으로 *forest(*포레스트*)*라고 합니다. 이 신뢰 관계는 도메인이 다양한 방법으로 서로의 리소스에 액세스하게 할 수 있습니다. 예를 들어 도메인 A에 정의된 사용자 계정은 도메인 B에 정의된 그룹의 멤버로 표시할 수 있습니다. management center는 ID 규칙을 위해 Active Directory 포리스트에서 사용자를 가져올 수 있습니다.
영역 시퀀스.	7.2.0	6.7.0	영역 시퀀스는 ID 규칙을 적용할 둘 이상의 영역으로 구성된 순서가 지정된 목록입니다. 영역 시퀀스를 ID 정책과 연결할 경우 Firepower System은 영역 시퀀스에 지정된 순서대로 Active Directory 도메인을 검색합니다. 신규/수정된 화면: **Integration(**통합**)** > **Other Integrations(**기타 통합**)** > **Realms(**영역**)** > **Realm Sequences(**영역 시퀀스**)**
사용자 제어를 위한 영역입니다.	7.2.0	모두	영역은 management center와 Active Directory 또는 LDAP 사용자 저장소 간의 연결입니다.