



## 영역 생성 및 관리

다음 주제에서는 사용자 인식 및 제어를 위한 사용자 저장소인, 영역을 생성하고 관리하는 방법을 설명합니다.

- [영역 및 영역 시퀀스 정보, 1 페이지](#)
- [영역 라이선스 요건, 5 페이지](#)
- [영역 요구 사항 및 사전 요건, 6 페이지](#)
- [영역 생성, 6 페이지](#)
- [영역 시퀀스 생성, 17 페이지](#)
- [영역 관리, 19 페이지](#)
- [영역 비교, 19 페이지](#)
- [영역 및 사용자 다운로드 문제 해결, 20 페이지](#)
- [영역 히스토리, 24 페이지](#)

## 영역 및 영역 시퀀스 정보

영역은 Firepower 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, 또는 ISE/ISE-PIC의 사용자 메타데이터에 대한 사용자 저장소를 쿼리합니다.

영역 시퀀스는 ID 정책에 사용할 두 개 이상의 영역으로 구성된 순서가 지정된 목록입니다. 영역 시퀀스를 ID 규칙과 연결할 경우 Firepower System은 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 Firepower Management Center이 서버를 쿼리할 때 저장한 변경 사항이 적용됩니다.

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

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

사용자 제어를 수행하려는 경우 다음을 구성할 수 있습니다.

- ISE/ISE-PIC용 AD 서버의 영역 또는 영역 시퀀스
- AD 서버 또는 캡티브 포털용 LDAP 서버의 영역 또는 영역 시퀀스

#### 사용자 다운로드 정보

Firepower Management Center과 LDAP 또는 AD 서버 간 연결을 구성하는 영역 또는 영역 시퀀스를 설정해 탐지한 특정 사용자에게 대한 사용자 및 사용자 그룹 메타데이터를 검색할 수 있습니다.

- 사용자 에이전트 또는 ISE/ISE-PIC에서 보고하거나 종속 포털을 통해 인증하는 LDAP 및 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.

영역에서 LDAP 서버나 Active Directory 도메인 컨트롤러 연결을 디렉터리로 설정할 수 있습니다. 사용자 인식 및 사용자 제어용으로 영역의 사용자 및 사용자 그룹 데이터를 다운로드하려면 **Download users and user groups for access control**(액세스 컨트롤을 위해 사용자 및 사용자 그룹 다운로드)을 선택해야 합니다.

Firepower Management Center에서는 각 사용자에게 대한 다음과 같은 정보 및 메타데이터를 얻습니다.

- LDAP 사용자 이름
- 이름 및 성
- 이메일 주소
- 부서
- 전화 번호

#### 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 Firepower Management Center 모델에 따라 달라집니다. 포함할 사용자 및 그룹을 선택할 때는 총 사용자 수가 모델 제한보다 작은지 확인하십시오. 액세스 컨트롤 파라미터가 너무 광범위하면, Firepower 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 Firepower Threat Defense* 명령 참조에 설명된 대로 **configure identity-subnet-filter** 명령을 사용할 수 있습니다.



**참고** 사용자 저장소에서 시스템이 탐지한 사용자를 제거할 경우, Firepower Management Center은(는) 절대 사용자 데이터베이스에서 해당 사용자를 제거하지 않습니다. 반드시 수동으로 삭제해야 합니다. 그러나 Firepower Management Center이(가) 신뢰할 수 있는 사용자 목록을 다음에 업데이트할 때 LDAP 변경 사항이 액세스 컨트롤 규칙에 반영됩니다.

비디오  [영역 만들기에 대한 YouTube 비디오.](#)

## 영역 및 신뢰할 수 있는 도메인

Firepower Management Center에서 영역을 구성하는 경우, 영역은 Active Directory 또는 LDAP 도메인에 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.

### Firepower System 및 신뢰할 수 있는 도메인

Firepower System은 신뢰할 수 있는 AD 도메인을 지원하지 않습니다. 즉 Firepower System은 설정한 어떤 도메인이 서로 신뢰하는지 추적하지 않으며, 어떤 도메인이 상위 또는 하위 도메인인지 알지 못합니다. 또한 Firepower System은 교차 도메인 신뢰를 이용하는 환경에 대한 지원을 보장하도록 테스트되지 않았으며, 신뢰 관계가 Firepower System 외부에서 실행되었다 하더라도 마찬가지입니다.

## 영역에 지원되는 서버

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

서버 유형	사용자 에이전트 데이터 검색용으로 지원되는지 여부	ISE 데이터 검색용으로 지원되는지 여부	캡티브 포털 데이터 검색용으로 지원되는지 여부	RA VPN 데이터 검색용으로 지원되는지 여부
Windows Server 2008 및 Windows Server 2012의 Microsoft Active Directory	예	예	예	예
Linux의 OpenLDAP	아니요	아니요	예	예

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
Linux의 OpenLDAP	아니요	아니요	예



**참고** TS 에이전트가 다른 패시브 인증 ID 소스(ISE/ISE-PIC)와 공유하는 Microsoft Active Directory Windows Server에 설치된 경우, Firepower Management Center는 TS 에이전트 데이터에 우선순위를 둡니다. TS 에이전트 및 수동 ID 소스가 동일한 IP 주소별로 활동을 보고할 경우, TS 에이전트 데이터만 Firepower 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 [MSDN](#)의 Active Directory 최대 제한 - 확장성을 참조하십시오.  
 필요한 경우 Active Directory 서버 구성을 수정하여 이러한 기본값 제한을 늘리고 더 많은 사용자를 수용할 수 있습니다.

## 지원되는 서버 개체 클래스 및 속성 이름

영역의 서버가 반드시 다음 표에 나와 있는 속성 이름을 사용해야 Firepower Management Center에서 해당 서버의 사용자 메타데이터를 검색합니다. 서버에서 속성 이름이 잘못된 경우 Firepower Management Center에서는 해당 속성의 정보를 데이터베이스에 입력할 수 없습니다.

표 1: Firepower Management Center 필드에 대한 속성 이름 지도

메타데이터	FMC 특성	LDAP ObjectClass	Active Directory 속성	OpenLDAP 속성
LDAP 사용자 이름	사용자 이름	<ul style="list-style-type: none"> <li>• user</li> <li>• inetOrgPerson</li> </ul>	samaccountname	cn uid
이름	First Name(이름)		givenname	givenname
last name(성)	Last Name(성)		sn	sn
email address(이메일 주소)	Email(이메일)		mail userprincipalname(메일에 값이 없는 경우)	mail
department	부서		department distinguishedname(부서에 값이 없는 경우)	ou
전화번호	전화번호		telephonenumber	telephonenumber



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

ObjectClasses 및 속성에 대한 자세한 내용은 다음 참조 자료를 참조하십시오.

- Microsoft Active Directory:
  - ObjectClasses: [MSDN](#)의 모든 클래스
  - Attributes: [MSDN](#)의 모든 속성
- OpenLDAP: [RFC 4512](#)

## 영역 라이선스 요건

**FTD** 라이선스  
Any(모든 상태)  
기본 라이선스  
제어

## 영역 요구 사항 및 사전 요건

모델 지원

모두

지원되는 도메인

모든

사용자 역할

- 관리자
- 액세스 관리자
- Network Admin(네트워크 관리자)

## 영역 생성

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

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

- [Active Directory 서버의 루트 인증서 내보내기, 13 페이지](#)
- [Active Directory 서버 이름 찾기, 12 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 사항](#)을 참조하십시오.

영역 디렉터리 설정 필드에 대한 자세한 내용은 [영역 필드, 7 페이지](#) 및 [영역 디렉터리 및 다운로드 동기화, 10 페이지](#)의 내용을 참조하십시오.



참고

모든 Microsoft Active Directory(AD) 영역에 대한 고유 **AD Primary Domain(AD 기본 도메인)**을 지정해야 합니다. 다른 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.

## 프로시저

- 
- 단계 1 Firepower Management Center에 로그인합니다.
- 단계 2 **System**(시스템) > **Integration**(통합) 버튼을 클릭합니다.
- 단계 3 **Realms**(영역)를 클릭합니다.
- 단계 4 새 영역을 생성하려면 **Add Realm**(영역 추가)을 클릭합니다.
- 단계 5 다른 작업(영역 활성화, 비활성화, 삭제 등)을 수행하는 방법은 [영역 관리, 19 페이지](#) 섹션을 참조하십시오.
- 단계 6 [영역 필드, 7 페이지](#)에 설명된 대로 영역 정보를 입력합니다.
- 단계 7 (선택 사항). **Test**(테스트)를 클릭해 영역에 대한 연결을 테스트합니다.
- 참고 Microsoft Active Directory 영역 테스트가 성공하려면, **AD Join Username**(AD 조인 사용자 이름)과 **AD Join Password**(AD 조인 비밀번호) 필드 모두에 값을 입력해야 하며 사용자는 컴퓨터를 도메인에 추가할 수 있는 권한이 있어야 합니다. 자세한 내용은 [영역 필드, 7 페이지](#)를 참고하십시오.
- 단계 8 **OK**(확인)를 클릭합니다.
- 단계 9 에 설명된 대로 [영역 디렉터리 설정, 15 페이지](#) 디렉터리를 한 개 이상 설정합니다.
- 단계 10 [사용자 및 그룹 다운로드, 16 페이지](#)에서 논의한 대로 사용자 및 사용자 그룹 다운로드(액세스 컨트롤에 필요)를 설정합니다.
- 단계 11 **Realm Configuration**(영역 설정)을 클릭합니다.
- 단계 12 **ISE/ISE-PIC Users**(ISE/ISE-PIC 사용자), **TS Agent Users**(TS 에이전트 사용자), **Captive Portal Users**(중속 포털 사용자), **Failed Captive Portal Users**(실패한 중속 포털 사용자), 및 **Guest Captive Portal Users**(게스트 중속 포털 사용자)에 대한 사용자 세션 시간 초과 값을 분 단위로 입력합니다.
- 단계 13 영역 설정을 완료했으면 **Save**(저장)를 클릭합니다.
- 

다음에 수행할 작업

- [영역 디렉터리 설정, 15 페이지](#)
- 영역을 편집, 삭제, 활성화 또는 비활성화합니다([영역 관리, 19 페이지](#) 참조).
- [영역 비교, 19 페이지](#)에 전달하는 고성능 고속 어플라이언스입니다.
- 필요한 경우 작업 상태를 모니터링합니다. [작업 메시지 보기](#)를 참조하십시오.

## 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**입니다. 지원되는 LDAP 저장소 목록은 [영역에 지원되는 서버, 3 페이지](#) 섹션을 참조하십시오. LDAP 리포지토리를 사용하여 중속 포털 사용자를 인증할 수 있습니다. 다른 모든 경우에는 Active Directory가 필요합니다.



참고 캡티브 포털만 LDAP 영역을 지원합니다.

### 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 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.

### 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.

- Microsoft Active Directory의 경우 사용자는 상승된 권한이 없어도 됩니다. 도메인에 어떤 사용자라도 지정할 수 있습니다.
- 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).

### Base DN(기본 DN)

Firepower 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)

Firepower Management Center이 그룹 속성으로 사용자를 검색해야 하는 서버의 디렉토리 트리입니다. 지원되는 그룹 속성 목록은 [지원되는 서버 개체 클래스 및 속성 이름](#), 4 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.

### Group Attribute(그룹 속성)

(선택 사항). 서버, 구성원 또는 고유 구성원의 그룹 속성입니다.

아래 필드는 기존 영역을 편집할 때만 사용할 수 있습니다.

#### 사용자 세션 시간 초과

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 Firepower Management Center가 Unknown(알 수 없음)으로 간주합니다(**Failed Captive Portal Users**(실패한 캡티브 포털 사용자) 제외).

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 소스](#)의 내용을 참조하십시오.

- 캡티브 포털 사용자: 캡티브 포털을 이용해 무사히 로그인한 사용자의 시간 초과 값으로, 액티브 인증의 유형입니다. 자세한 내용은 [캡티브 포털 ID 소스](#)를 참고하십시오.
- 실패한 캡티브 포털 사용자: 캡티브 포털을 사용하여 무사히 로그인하지 못한 사용자의 시간 초과 값입니다. Firepower Management Center가 사용자를 Failed Auth User(실패한 인증 사용자)로 간주하기 전의 최대 로그인 시도 횟수를 설정할 수 있습니다. Failed Auth User(실패

한 인증 사용자는 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 소스](#)를 참고하십시오.

## 영역 디렉토리 및 다운로드 동기화

### 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, 12 페이지](#)의 내용을 참조하십시오.

#### 포트

Firepower Management Center와 컨트롤러를 연결하는 데 사용할 포트입니다.

#### 암호화

(적극 권장함.) Firepower Management Center와 서버를 연결하는 데 사용할 암호화 방법입니다.

- **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, 12 페이지](#)의 내용을 참조하십시오.

#### SSL 인증서

서버에 인증하는 데 사용할 SSL 인증서입니다. 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.

#### 사용자 **Download(다운로드)** 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 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.

**Download users and groups**(사용자 및 그룹 다운로드)(사용자 액세스 제어의 필수 사항)

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

**Begin automatic download at, Repeat every**(자동 다운로드 시작 기준, 반복 빈도)

자동 다운로드의 빈도를 지정합니다.

지금 다운로드

그룹 및 사용자를 AD와 동기화하려면 클릭합니다.

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

정책에서 사용할 수 있는 그룹을 제한합니다.

- 그룹을 **Add to Include**(포함에 추가) 또는 **Add to Exclude**(제외에 추가) 필드로 이동하지 않는 한 **Available Groups**(사용 가능한 그룹) 필드에 표시되는 그룹은 정책에 사용할 수 있습니다.
- 그룹을 **Add to Include**(포함에 추가) 필드로 이동하면 이러한 그룹만 다운로드되고 사용자 데이터를 사용자 인식 및 사용자 제어에 사용할 수 있습니다.
- 그룹을 **Add to Exclude**(제외에 추가) 필드로 이동하면 이러한 그룹을 제외한 모든 그룹이 다운로드되고 사용자 데이터를 사용자 인식 및 사용자 제어에 사용할 수 있습니다.
- 포함되지 않은 그룹에 있는 사용자를 포함하려면, 아래 **Groups to Include**(포함할 그룹) 필드에 사용자 이름을 입력하고 **Add**(추가)를 클릭합니다.
- 제외되지 않은 그룹에 있는 사용자를 제외하려면, 아래 **Groups to Exclude**(제외할 그룹) 필드에 사용자 이름을 입력하고 **Add**(추가)를 클릭합니다.



참고 Firepower 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.

다음 위치에서 자동 다운로드 시작  
AD에서 사용자 및 그룹을 다운로드할 시간 및 시간 간격을 입력합니다.

## Active Directory에 안전하게 연결

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

- Active Directory 서버의 루트 인증서를 내보냅니다.
- 신뢰할 수 있는 인증서 저장소로 루트 인증서를 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](#), 13 페이지

[Active Directory 서버 이름 찾기](#), 12 페이지

[영역 디렉터리 설정](#), 15 페이지

## Active Directory 서버 이름 찾기

FMC에서 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

영역 디렉터리를 생성합니다.

관련 항목

[Active Directory 서버의 루트 인증서 내보내기](#), 13 페이지

## Active Directory 서버의 루트 인증서 내보내기

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

시작하기 전에

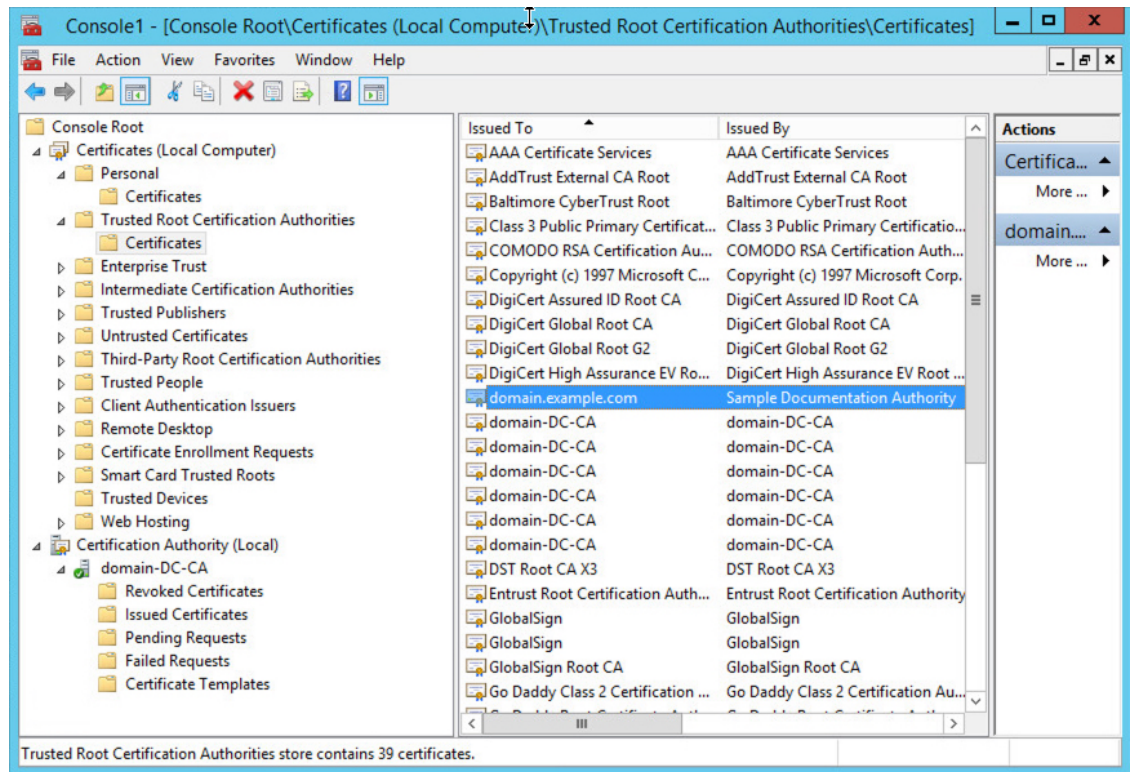
Active Directory 서버 루트 인증서의 이름을 알아야 합니다. 루트 인증서의 이름이 도메인과 같거나 인증서의 이름이 다를 수 있습니다. 다음 절차에서는 이름을 찾을 수 있는 한 가지 방법을 보여줍니다. 다른 방법이 있을 수도 있습니다

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 2012만 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 FMC에 연결할 수 있는 경우 인증서를 내보내는 편리한 방법입니다.

- Start**(시작)를 클릭하고 **cmd**를 입력합니다.
- certutil -ca.cert certificate-name** 명령을 입력합니다.  
서버의 인증서가 화면에 표시됩니다.
- 전체 인증서를 클립 보드에 복사합니다. **-----BEGIN CERTIFICATE-----**(으)로 시작하여 **-----END CERTIFICATE-----**(으)로 끝냅니다(해당 문자열 포함).

다음에 수행할 작업

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

관련 항목

[Active Directory 서버 이름 찾기](#), 12 페이지

## 영역 디렉터리 설정

이 절차를 이용하면 영역 디렉터리를 생성할 수 있으며, 이 디렉터리는 LDAP 서버 또는 Microsoft Active Directory 도메인 컨트롤러에 해당합니다. Active Directory 서버는 여러 도메인 컨트롤러를 보유할 수 있으며, 각 컨트롤러는 서로 다른 사용자 및 그룹을 인증할 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 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 사항](#)을 참조하십시오.

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

영역 디렉터리 설정 필드에 대한 자세한 내용은 [영역 필드, 7 페이지](#)을(를) 참고하십시오.

시작하기 전에

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

- [Active Directory 서버의 루트 인증서 내보내기, 13 페이지](#)
- [Active Directory 서버 이름 찾기, 12 페이지](#)

프로시저

- 
- 단계 1 아직 수행하지 않았다면 Firepower Management Center에 로그인하고 **System(시스템) > Integration(통합) > Realms(영역)**를 클릭합니다.
  - 단계 2 **Realms(영역)** 페이지에서 디렉터리를 설정할 영역의 이름을 클릭합니다.
  - 단계 3 **Directory(디렉터리)** 페이지에서 **Add Directory(디렉터리 추가)**를 클릭합니다.
  - 단계 4 LDAP 서버 또는 Active Directory 도메인 컨트롤러의 **Hostname / IP Address(호스트 이름/IP 주소)**와 **Port(포트)**를 입력합니다.  
시스템은 LDAP 쿼리를 사용자가 지정한 호스트 이름이나 IP 주소로 보냅니다. 호스트 이름이 LDAP 서버 또는 Active Directory 도메인 컨트롤러의 IP 주소로 확인된다면, **Test(테스트)**는 성공하게 됩니다.
  - 단계 5 **Encryption Mode(암호화 모드)**를 선택합니다.
  - 단계 6 목록에서 **SSL Certificate(SSL 인증서)**를 선택하거나 추가(+)**를 클릭하여 인증서를 추가합니다.**
  - 단계 7 연결을 테스트하려면 **Test(테스트)**를 클릭합니다.
  - 단계 8 **OK(확인)**를 클릭합니다.
  - 단계 9 **Save(저장)**를 클릭합니다. **Realms(영역)** 페이지로 돌아옵니다.
  - 단계 10 영역을 아직 활성화하지 않았다면 **Realms(영역)** 페이지에서 **State(상태)**를 활성화쪽으로 밍니다.
-

다음에 수행할 작업

- [사용자 및 그룹 다운로드, 16 페이지](#)에 전달하는 고성능 고속 어플라이언스입니다.

관련 항목

[Active Directory 서버의 루트 인증서 내보내기, 13 페이지](#)

[Active Directory 서버 이름 찾기, 12 페이지](#)

[영역 시퀀스 생성, 17 페이지](#)

## 사용자 및 그룹 다운로드

스마트 라이선스	기본 라이선스	지원되는 장치	지원되는 도메인	액세스
Any(모든)	제어	Any(모든)	Any(모든)	관리자, 액세스 관리자, 네트워크 관리자

이 섹션은 Active Directory 서버의 사용자와 그룹을 Firepower Management Center로 다운로드하는 방법을 설명합니다. 포함할 그룹을 지정하지 않으면 시스템은 제공된 매개변수와 일치하는 모든 그룹에 대한 사용자 데이터를 검색합니다. 성능상의 이유로 Cisco에서는 액세스 제어에서 사용하려는 사용자를 나타내는 그룹만 명시적으로 포함할 것을 권장합니다.


Firepower Management Center이(가) 서버에서 검색할 수 있는 최대 사용자 수는 Firepower Management Center 모델에 따라 다릅니다. 영역의 다운로드 매개변수 범위가 너무 넓으면 Firepower Management Center에서는 최대한 많은 사용자의 정보를 가져오며, 가져오는 데 실패한 사용자 수를 Message Center(메시지 센터)의 Task(작업)에 보고합니다.


영역 컨피그레이션 필드에 대한 자세한 내용은 [영역 필드, 7 페이지](#)를 참고하십시오.

프로시저

단계 1 Firepower Management Center에 로그인합니다.

단계 2 **System**(시스템) > **Integration**(통합) > **Realms**(영역)를 클릭합니다.

단계 3 사용자 및 그룹을 수동으로 다운로드하려면 영역 옆에 있는 다운로드()를 클릭하여 사용자와 사용자 그룹을 다운로드합니다. 컨트롤이 흐리게 표시되는 경우에는 컨피그레이션이 상위 도메인에 속하거나 컨피그레이션을 수정할 권한이 없는 것입니다. 이 절차의 나머지 부분은 건너뛰어도 됩니다.

단계 4 자동 사용자 및 그룹 다운로드에 대한 영역을 설정하려면 자동 사용자 및 그룹 다운로드에 설정할 영역 옆에 있는 편집()을 클릭합니다.

단계 5 User Access Control(사용자 액세스 제어) 페이지에서 **Download users and groups (required for user access control)**(사용자 및 그룹 다운로드)(사용자 액세스 제어의 필수 사항)를 확인합니다.

단계 6 목록에서 **Begin automatic download at**(자동 다운로드 시작 기준)의 시간을 선택합니다.

단계 7 **Repeat Every**(반복 빈도) 목록에서 다운로드 간격을 선택합니다.



**단계 8** 다운로드에서 사용자 그룹을 포함하거나 제외하려면 **Available Groups**(사용 가능한 그룹) 열에서 사용자 그룹을 선택하고 **Add to Include**(포함에 추가) 또는 **Add to Exclude**(제외에 추가)를 클릭합니다. 사용자가 여러 명인 경우 쉼표로 구분하십시오. 또한 이 필드에서 와일드카드 문자로 별표(\*)를 사용할 수 있습니다.

참고 해당 그룹의 사용자에게 대해 사용자 제어를 수행하려면 **Add to Include**(포함에 추가)를 선택해야 합니다.

다음 지침을 사용하십시오.

- **Available Groups**(사용 가능한 그룹) 상자에 그룹을 그대로 두면 해당 그룹이 다운로드되지 않습니다.
- 그룹을 **Add to Include**(포함에 추가) 상자로 이동하면 그룹이 다운로드되고 사용자 데이터를 사용자 인식 및 사용자 제어에 사용할 수 있습니다.
- 그룹을 **Add to Exclude**(제외에 추가) 상자로 이동하면 그룹이 다운로드되고 사용자 데이터를 사용자 인식에 사용할 수 있으나, 사용자 제어에는 사용할 수 없습니다.
- 포함되지 않은 그룹에 있는 사용자를 포함하려면, 아래 **Groups to Include**(포함할 그룹) 필드에 사용자 이름을 입력하고 **Add**(추가)를 클릭합니다.
- 제외되지 않은 그룹에 있는 사용자를 제외하려면, 아래 **Groups to Exclude**(제외할 그룹) 필드에 사용자 이름을 입력하고 **Add**(추가)를 클릭합니다.

## 영역 시퀀스 생성

다음 절차를 수행하면 Firepower System에서 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 Firepower System이 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.

- **영역 디렉터리 설정, 15 페이지**에 설명된 대로 디렉터리를 생성합니다.
- **사용자 및 그룹 다운로드, 16 페이지**에 설명된 대로 사용자 및 그룹을 다운로드하고 영역을 활성화합니다.

프로시저

**단계 1** 아직 하지 않았다면 Firepower Management Center에 로그인합니다.

- 단계 2 **System**(시스템) > **Integration**(통합) > **Realms Sequences**(영역 시퀀스)를 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 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 **Firepower System**이 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 생성](#)의 내용을 참조하십시오.

관련 항목





[영역 디렉터리 설정](#), 15 페이지

## 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.
- 보기 (  )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

### 프로시저

- 
- 단계 1 Firepower Management Center에 로그인합니다.
  - 단계 2 **System(시스템) > Integration(통합)** 버튼을 클릭합니다.
  - 단계 3 **Realms(영역)**를 클릭합니다.
  - 단계 4 영역을 삭제하려면 삭제(  )을 클릭합니다.
  - 단계 5 영역을 편집하려면 영역 옆의 수정(  )을 클릭하고 [영역 생성, 6 페이지](#)에 설명된 대로 영역을 변경합니다.
  - 단계 6 영역을 활성화하려면 **State(상태)**를 오른쪽으로 끄십시오. 영역을 비활성화하려면 왼쪽으로 끄십시오.
  - 단계 7 사용자 및 사용자 그룹을 다운로드하려면 다운로드(  )을 클릭합니다.
  - 단계 8 영역을 복사하려면 복사(  )을 클릭합니다.
  - 단계 9 영역을 비교하려면 [영역 비교, 19 페이지](#)를(를) 참고하십시오.
- 

## 영역 비교

이 작업을 수행하려면 관리자, 액세스 관리자, Network Admin(네트워크 관리자) 또는 보안 승인자이어야 합니다.

### 프로시저

- 
- 단계 1 Firepower Management Center에 로그인합니다.
  - 단계 2 **System(시스템) > Integration(통합)** 버튼을 클릭합니다.
  - 단계 3 **Realms(영역)**를 클릭합니다.
  - 단계 4 **System(시스템) > Integration(통합)** 버튼을 클릭합니다.
  - 단계 5 **Realms(영역)**를 클릭합니다.

- 단계 6 **Compare Realms**(영역 비교)를 클릭합니다.
- 단계 7 **Compare Against**(비교 대상) 목록에서 **Compare Realm**(영역 비교)을 선택합니다.
- 단계 8 **Realm A**(영역 A) 및 **Realm B**(영역 B) 목록에서 비교할 영역을 선택합니다.
- 단계 9 **OK**(확인)를 클릭합니다.
- 단계 10 변경 사항을 개별적으로 탐색하려면 제목 표시줄 위의 **Previous**(이전) 또는 **Next**(다음)를 클릭합니다.
- 단계 11 (선택 사항). **Comparison Report**(비교 보고서)를 클릭하여 영역 비교 보고서를 생성합니다.
- 단계 12 (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](#)
- [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

Firepower Management Center의 상태 모니터는 사용자 또는 영역의 불일치를 알려주며, 이러한 불일치는 다음과 같이 정의됩니다.

- 사용자 불일치: 사용자가 다운로드되지 않고 Firepower Management Center에 보고됩니다.  
사용자 불일치가 발생하는 일반적인 이유는 사용자가 Firepower Management Center 다운로드에서 제외된 그룹에 속하기 때문입니다. [영역 필드, 7 페이지](#)에서 논의된 정보를 검토합니다.
- 영역 불일치: 사용자가 Firepower Management Center의 알 수 없는 영역에 해당하는 도메인에 로그인합니다.

예를 들어 Firepower Management Center의 **domain.example.com**(이)라는 도메인에 대응하는 영역을 정의했지만 로그인인 **another-domain.example.com**(이)라는 도메인에서 보고되었다면, 이것은 영역 불일치가 됩니다. 이 도메인의 사용자는 Firepower 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, 23 페이지](#)를 참고하십시오.

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, **Firepower**는 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 **Firepower** 액세스 제어 정책 규칙이 일치하지 않습니다.

솔루션: 도메인 컨트롤러 1에 유사한 그룹을 생성합니다. 여기에는 그룹 A에 속한 모든 도메인 1 어 카운트가 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, **Firepower**는 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**(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 조인 사용자 이름)과 **AD Join Password**(AD 조인 비밀번호)가 올바릅니다.  
**AD Join Username**(AD 조인 사용자 이름)은 온전한 이름이어야 합니다(예: **administrator**가 아닌 **administrator@mydomain.com**).
- 사용자는 도메인에서 컴퓨터를 생성하고 Firepower Management Center를 도메인에 도메인 컴퓨터로 조인할 권한을 가집니다.

증상: 예기치 않은 시간에 사용자 시간 초과가 발생함

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

증상: 영역 설정에 지정된 대로 사용자가 포함되지 않거나 제외됨

서버에 있는 하위 그룹의 구성원인 사용자를 포함하거나 제외하는 Active Directory 영역을 구성할 경우, Microsoft Windows 서버는 보고하는 사용자 수를 제한합니다.

- Microsoft Windows Server 2012의 그룹당 사용자 수 5,000명

필요한 경우, 서버 컨피그레이션을 수정하여 이러한 기본값 제한을 늘리고 더 많은 사용자를 수용할 수 있습니다.

증상: 사용자가 다운로드되지 않음

가능한 원인은 다음과 같습니다.

- 영역 **Type**(유형)을 잘못 설정한 경우, 사용자와 그룹을 다운로드할 수 없습니다. Firepower System이 기대하는 속성과 저장소가 제공하는 속성이 일치하지 않기 때문입니다. 예를 들어 Microsoft Active Directory 영역의 **Type**(유형)을 **LDAP**로 설정하면, Firepower System은 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.

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

데이터베이스에 데이터가 아직 없는 **ISE** 사용자의 활동이 탐지되면 시스템은 서버에서 관련된 정보를 검색합니다. **Active Directory** 서버에서 이러한 정보를 정상적으로 검색하기까지 추가 시간이 필요한 경우도 있습니다. 데이터 검색에 성공할 때까지 **ISE** 또는 사용자 에이전트 사용자에 의해 확인된 활동이 웹 인터페이스에 표시되지 않습니다.

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.

## 영역 또는 사용자 불일치 탐지

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

- 사용자 불일치: 사용자가 다운로드되지 않고 **Firepower Management Center**에 보고됩니다.  
사용자 불일치가 발생하는 일반적인 이유는 사용자가 **Firepower Management Center** 다운로드에서 제외된 그룹에 속하기 때문입니다. **영역 필드, 7 페이지**에서 논의된 정보를 검토합니다.
- 영역 불일치: 사용자가 **Firepower Management Center**의 알 수 없는 영역에 해당하는 도메인으로 로그인합니다.

자세한 정보는 **영역 및 사용자 다운로드 문제 해결, 20 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 **Firepower Management Center**에 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, 20 페이지](#)를 참고하십시오.

g) 페이지 하단의 **Save Policy & Exit(정책 저장 및 종료)**를 클릭합니다.

h) **상태 정책 적용**에 설명된 대로 상태 정책을 매니지드 디바이스에 적용합니다.

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

- 경고 임계값을 초과한 경우, Firepower 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.

관련 항목

[상태 정책](#)

[상태 모니터링 구성](#)

[상태 모니터 상태 카테고리](#)

## 영역 히스토리

기능	버전	세부 사항
영역 시퀀스	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.
사용자 제어를 위한 영역입니다.	—	버전 6.0 이전에 도입된 기능. 영역은 FMC와 Active Directory 또는 LDAP 사용자 저장소 간의 연결입니다.