



## ID 정책 생성 및 관리

다음 주제는 ID 규칙과 ID 정책을 만들고 관리하는 방법을 설명합니다.

- ID 정책 정보, 1 페이지
- ID 정책 라이선스 요구 사항, 2 페이지
- ID 정책 요구 사항 및 사전 요건, 2 페이지
- ID 규칙 생성, 3 페이지
- ID 정책 생성, 6 페이지
- ID 규칙 관리, 7 페이지
- ID 정책 관리, 8 페이지

## ID 정책 정보

ID 정책에는 ID 규칙이 포함됩니다. ID 규칙은 트래픽 집합을 영역 및 인증 방법(패시브 인증, 활성 인증, 인증 없음)과 연결합니다.

다음 단락에서 언급하는 예외 사항이 아닌 이상, 사용하려는 영역과 인증 방법을 먼저 설정해야 ID 규칙에서 이를 호출할 수 있습니다.

- ID 정책 외부, **System(시스템) > Integration(통합) > Realms(영역)**에서 영역을 설정합니다. 자세한 내용은 [영역 생성](#)를 참고하십시오.
- **System(시스템) > Integration(통합) > Identity Sources(ID 소스)**에서 인 사용자 에이전트와 를 설정합니다. 자세한 내용은 [사용자 제어를 위한 ISE/ISE-PIC 설정](#)를 참조하십시오.
- ID 정책 내에서 액티브 인증 ID 소스인 캡티브 포털을 설정합니다. 자세한 내용은 [사용자 제어에 대한 캡티브 포털 설정 방법](#)를 참고하십시오.
- Remote Access VPN 정책에서 액티브 인증 ID 소스인 Remote Access VPN을 설정합니다. 자세한 내용은 [Remote Access VPN 인증](#)를 참고하십시오.

여러 ID 규칙을 단일 ID 정책에 추가한 후, 규칙 순서를 지정합니다. 시스템은 오름차순 규칙 번호에 따라 하향식 순서로 트래픽이 규칙과 일치하는지를 확인합니다. 트래픽에 일치하는 첫 번째 규칙이 트래픽을 처리하는 규칙입니다.

하나 이상의 ID 정책을 설정한 후에는 ID 정책 하나를 액세스 컨트롤 정책에 연결해야 합니다. 네트워크의 트래픽이 ID 규칙의 조건과 일치하면, 시스템은 트래픽을 지정된 영역과 연결하며 지정된 ID 소스를 사용하여 트래픽의 사용자를 인증합니다.

ID 정책을 구성하지 않으면 시스템은 사용자 인증을 수행하지 않습니다.

#### ID 정책 생성 예외 사항

ID 정책은 다음이 모두 참인 경우 필요하지 않습니다.

- ISE/ISE-PIC ID 소스를 사용합니다.
- 액세스 제어 정책에서 사용자 또는 그룹을 사용하지 않습니다.
- 액세스 제어 정책에서 SGT(Security Group Tag)를 사용합니다. 자세한 내용은 [ISE SGT 및 맞춤형 SGT 규칙 조건 비교](#)를 참고하십시오.

비디오  ID 정책 및 규칙 생성에 대한 YouTube 비디오.

관련 항목

[ID 정책 설정 방법](#)

## ID 정책 라이선스 요구 사항

**FTD** 라이선스

Any(모든 상태)

기본 라이선스

제어

## ID 정책 요구 사항 및 사전 요건

모델 지원

모두

지원되는 도메인

모든

사용자 역할

- 관리자
- 액세스 관리자

- Network Admin(네트워크 관리자)

## ID 규칙 생성

ID 규칙의 설정 옵션에 대한 자세한 내용은 [Identity Rule Fields\(ID 규칙 필드\)](#), 4 페이지 섹션을 참조하십시오.

시작하기 전에

영역 또는 영역 시퀀스를 생성하고 활성화해야 합니다.

- [영역 생성](#)에 설명된 대로 를 생성합니다.
- (선택 사항). [영역 시퀀스 생성](#)에 설명된 대로 영역 시퀀스를 생성합니다.
- [영역 디렉터리 설정](#)에 설명된 대로 디렉터리를 생성합니다.
- [사용자 및 그룹 다운로드](#)에 설명된 대로 사용자 및 그룹을 다운로드하고 영역을 활성화합니다.

프로시저

단계 1 아직 하지 않았다면 Firepower Management Center에 로그인합니다.

단계 2 **Policies(정책) > Access Control(액세스 제어) > Identity(ID)** 버튼을 클릭합니다.

단계 3 ID 규칙을 추가할 ID 정책 옆에 있는 수정(✎)을 클릭합니다.

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

단계 4 **Add Rule(규칙 추가)**을 클릭합니다.

단계 5 **Name(이름)**을 입력합니다.

단계 6 규칙이 **Enabled(활성화)** 상태인지 여부를 지정합니다.

단계 7 기존 카테고리에 규칙을 추가하려면 규칙을 **Insert(삽입)**할 위치를 나타냅니다. 새 카테고리를 추가하려면 **Add Category(카테고리 추가)**를 클릭합니다.

단계 8 목록에서 규칙 **Action(작업)**을 선택합니다.

단계 9 **Realms & Settings(영역 및 설정)**를 클릭합니다.

단계 10 **Realms(영역)** 목록에서 ID 규칙에 대한 영역 또는 영역 시퀀스를 선택합니다. 영역 또는 영역 시퀀스를 모든 ID 규칙과 연결해야 합니다.

영역 요구사항의 유일한 예외는 ISE SGT 속성 태그만 사용하여 사용자 제어를 구현하는 것입니다. 이 경우에는 ISE 서버에 대한 영역 또는 영역 시퀀스는 설정하지 않아도 됩니다. 연결된 ID 정책이 포함되어 있거나 포함되지 않은 정책에서 ISE SGT 속성 조건을 설정할 수 있습니다.

단계 11 캡티브 포털을 설정하는 경우에는 [사용자 제어에 대한 캡티브 포털 설정 방법](#) 섹션을 참조하십시오.

단계 12 (선택사항) ID 규칙에 조건을 추가하려면 [규칙 조건 유형](#) 섹션을 참조하십시오.

단계 13 **Add**(추가)를 클릭합니다.

단계 14 정책 편집기에서 규칙 위치를 설정합니다. 이렇게 하려면 규칙을 클릭하여 끌거나 오른쪽 클릭 메뉴를 사용하여 잘라내고 붙여넣습니다. 규칙은 번호가 지정되며 1부터 시작합니다. 시스템은 오름차순 규칙 번호에 따라 하향식 순서로 트래픽이 규칙과 일치하는지를 확인합니다. 트래픽에 일치하는 첫 번째 규칙이 트래픽을 처리하는 규칙입니다. 규칙 순서가 올바르면 네트워크 트래픽 처리에 필요한 리소스가 줄어들면서 규칙 선점이 방지됩니다.

단계 15 **Save**(저장)를 클릭합니다.

## Identity Rule Fields(ID 규칙 필드)

ID 규칙을 구성하려면 다음 필드를 사용합니다.

### Enabled(활성화)

이 옵션을 선택하면 ID 정책에서 ID 규칙이 활성화됩니다. 이 옵션을 선택 취소하면 ID 규칙이 비활성화됩니다.

### 작업

지정한 영역에 있는 사용자에게 대해 실행할 인증 유형을 지정합니다. **Passive Authentication**(패시브 인증)(기본값), **Active Authentication**(액티브 인증) 또는 **No Authentication**(인증 없음)을 지정할 수 있습니다. 인증 방법, 즉 ID 소스를 완전히 구성해야 ID 규칙에서 이를 작업으로 선택할 수 있습니다.

또한 VPN이 활성화된 경우(최소 하나 이상의 매니지드 디바이스에서 구성됨) **Remote Access VPN** 세션은 VPN에 의해 액티브 인증됩니다. 다른 세션은 규칙 작업을 사용합니다. 즉, VPN이 활성화되면 선택한 작업에 관계없이 모든 세션에 대해 VPN ID 확인이 먼저 수행됩니다. 지정된 영역에 VPN ID가 있을 경우, 이를 ID 소스로 사용합니다. **No additional captive portal active authentication is done, even if selected.**

VPN ID 소스가 없는 경우, 지정된 작업에 따라 프로세스가 계속 진행됩니다. VPN ID 소스가 없는 경우 ID 정책을 VPN 인증에만 제한할 수 없으며, 선택한 작업에 따라 규칙이 적용됩니다.



주의 SSL 암호 해독이 비활성화되어 있을 때(액세스 컨트롤 정책에 SSL 정책이 포함되지 않을 때) 첫 번째 액티브 인증을 추가하거나 마지막 액티브 인증을 제거할 컨피그레이션 변경 사항을 구축할 때 Snort 프로세스가 재시작되므로 트래픽 검사가 일시적으로 중단됩니다. 이 중단 기간 동안 트래픽이 삭제되는지 아니면 추가 검사 없이 통과되는지는 대상 디바이스가 트래픽을 처리하는 방법에 따라 달라집니다. 자세한 내용은 **Snort® 재시작 트래픽 동작**을 참고하십시오.

액티브 인증 규칙에는 **Active Authentication**(액티브 인증) 규칙 작업 또는 **Use active authentication if passive or VPN identity cannot be established**(패시브 또는 VPN ID를 설정할 수 없는 경우 활성 인증 사용)가 선택된 **Passive Authentication**(패시브 인증) 규칙 작업이 있음에 유의하십시오.

현재 보유한 버전의 Firepower System에서 어떤 수동 및 액티브 인증 방법을 지원하는지에 대한 내용은 **사용자 ID 소스 정보**를 참조하십시오.

**Realm(영역)**

지정된 **Action(작업)**을 수행할 사용자가 포함된 영역 또는 영역 시퀀스. 영역 또는 영역 시퀀스를 완전히 설정해야 ID 규칙에서 이를 영역으로 선택할 수 있습니다.



참고 원격 액세스 VPN이 활성화되어 있고 구축에서 VPN 인증에 RADIUS 서버 그룹을 사용할 경우, 이 RADIUS 서버 그룹과 연결된 영역을 지정하십시오.



참고 **Kerberos**(Kerberos를 옵션으로 사용하려는 경우에는 **HTTP Negotiate(HTTP 협상)**)를 ID 규칙의 **Authentication Protocol(인증 프로토콜)**로 선택할 경우, Kerberos 캡티브 포털(captive portal) 액티브 인증을 수행하려면 선택한 **Realm(영역)**에 **AD Join Username(AD 조인 사용자 이름)**과 **AD Join Password(AD 조인 비밀번호)**를 구성해야 합니다.

**Use active authentication if passive or VPN identity cannot be established(패시브 인증 또는 VPN ID를 설정할 수 없는 경우 액티브 인증 사용)**

패시브 또는 VPN 인증이 사용자를 식별하지 못할 경우, 이 옵션을 선택하면 캡티브 포털(captive portal) 액티브 인증을 통해 사용자를 인증합니다. 이 옵션을 선택하려면 ID 정책에서 캡티브 포털(captive portal) 액티브 인증을 구성해야 합니다.

이 옵션을 비활성화하면 VPN ID가 없거나 패시브 인증으로 식별할 수 없는 사용자는 Unknown(알 수 없음)으로 식별됩니다.

**인증에서 사용자를 식별할 수 없는 경우 특수 ID/게스트로 식별함**

이 옵션을 선택하면 지정된 횟수만큼 캡티브 포털(captive portal) 액티브 인증에 실패한 사용자가 네트워크에 게스트로 액세스할 수 있습니다. Firepower Management 콘솔에 표시되는 이러한 사용자는 사용자 이름(사용자 이름이 AD 또는 LDAP 서버에 있는 경우) 또는 **Guest(게스트)**(사용자 이름을 알 수 없는 경우)로 식별됩니다. 이 영역은 ID 규칙에 지정된 영역입니다. (기본 로그인 실패 횟수는 3회입니다.)

이 필드는 **Active Authentication(액티브 인증)**(즉 캡티브 포털 인증)을 규칙 **Action(작업)**으로 설정했을 때만 표시됩니다.

**Authentication Protocol(인증 프로토콜)**

캡티브 포털 액티브 인증을 수행하는 데 사용할 방법입니다. 선택 사항은 영역의 유형, LDAP 또는 AD에 따라 달라집니다.

- 암호화되지 않은 HTTP BA(Basic Authentication) 연결을 사용하여 사용자를 인증하려는 경우 **HTTP Basic(HTTP 기본)**을 선택합니다. 사용자는 브라우저의 기본 인증 팝업 창을 통해 네트워크에 로그인합니다.

대부분의 웹 브라우저는 **HTTP Basic(HTTP 기본)** 로그인의 접속 정보를 캐시하며, 접속 정보를 사용하여 기존 세션의 시간이 초과하면 새 세션을 원활하게 시작합니다.

- NTLM(NT LAN Manager) 연결을 사용하여 사용자를 인증하려는 경우 **NTLM**을 선택합니다. 이 선택 사항은 AD 영역을 선택한 경우에만 사용 가능합니다. 사용자의 브라우저에 투명 인증이 구성된 경우, 사용자는 자동으로 로그인됩니다. 투명 인증이 구성되지 않은 경우, 사용자는 브라우저의 기본 인증 팝업 창을 통해 네트워크에 로그인합니다.
- 캡티브 포털(captive portal) 서버가 인증 연결에 HTTP Basic(HTTP 기본) 또는 NTLM 중에서 선택할 수 있도록 하려면 **HTTP Negotiate(HTTP 협상)**를 선택합니다. 이 선택 사항은 AD 영역을 선택한 경우에만 사용 가능합니다.



**참고** HTTP 협상 캡티브 포털(captive portal)을 수행할 ID 규칙을 생성 중이고 DNS 확인을 구성한 경우, 캡티브 포털(captive portal) 디바이스의 FQDN(Fully Qualified Domain Name)을 확인할 DNS 서버를 구성해야 합니다. FQDN은 DNS를 구성할 때 제공된 호스트 이름과 일치해야 합니다.

ASA with FirePOWER Services, FQDN은 캡티브 포털(captive portal)에 사용된 라우팅 인터페이스의 IP 주소를 확인해야 합니다.

## ID 정책 생성

### 시작하기 전에

액세스 컨트롤 정책의 영역에서 사용자와 그룹을 사용하려면 ID 정책이 있어야 합니다. [영역 생성](#)에 설명된 대로 하나 이상의 영역을 생성하고 활성화합니다.

ID 정책은 다음이 모두 참인 경우 필요하지 않습니다.

- ISE/ISE-PIC ID 소스를 사용합니다.
- 액세스 제어 정책에서 사용자 또는 그룹을 사용하지 않습니다.
- 액세스 제어 정책에서 SGT(Security Group Tag)를 사용합니다. 자세한 내용은 [ISE SGT 및 맞춤형 SGT 규칙 조건 비교](#)를 참고하십시오.

### 프로시저

단계 **1** Firepower Management Center에 로그인합니다.

단계 **2** **Policies(정책) > Access Control(액세스 제어) > Identity(ID)** 을(를) 클릭하고 **New Policy(새로운 정책)** 를 클릭합니다.

단계 **3** **Name(이름)**을 입력하고 필요한 경우, **Description(설명)**을 입력합니다.

단계 **4** **Save(저장)**를 클릭합니다.

단계 **5** 정책에 규칙을 추가하려면 **ID 규칙 생성, 3 페이지**에 설명된 대로 **Add Rule(규칙 추가)**을 클릭합니다.

단계 6 규칙 카테고리를 생성하려면 **Add Category**(카테고리 추가)를 클릭합니다.

단계 7 종속 포털 액티브 인증을 설정하려면 **캡티브 포털 설정 1부: ID 정책 생성**에 설명된 대로 **Active Authentication**(액티브 인증)을 클릭합니다.

단계 8 **Save**(저장)를 클릭하여 ID 정책을 저장합니다.

다음에 수행할 작업

- 일치시킬 사용자를 지정하는 ID 정책과 기타 옵션을 규칙에 추가합니다([ID 규칙 생성, 3 페이지 참조](#)).
- ID 정책을 액세스 컨트롤 정책에 연결해 선택한 사용자가 지정된 리소스에 액세스하도록 허용하거나 액세스하지 못하게 합니다([액세스 제어에 다른 정책 연결 참조](#)).
- 매니지드 디바이스에 설정 변경사항을 구축합니다([컨피그레이션 변경 사항 구축 참조](#)).

문제가 발생하는 경우에는 [사용자 제어 문제 해결](#) 섹션을 참조하십시오.

관련 항목

[캡티브 포털 설정 1부: ID 정책 생성](#)

[캡티브 포털\(captive portal\) 필드](#)

[사용자 제어 문제 해결](#)

## ID 규칙 관리

프로시저

단계 1 아직 하지 않았다면 Firepower Management Center에 로그인합니다.

단계 2 **Policies**(정책) > **Access Control**(액세스 제어) > **Identity(ID)** 버튼을 클릭합니다.

단계 3 수정하려는 정책 옆에 있는 수정(✍)를 클릭합니다. 보기(👁)이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

단계 4 ID 규칙을 수정하려면 수정(✍)을 클릭하고 **ID 정책 생성, 6 페이지**에 설명된 대로 규칙을 변경합니다.

단계 5 ID 규칙을 삭제하려면 삭제(🗑)을 클릭합니다.

단계 6 규칙 카테고리를 생성하려면 **Add Category**(카테고리 추가)를 클릭하고 위치와 규칙을 선택합니다.

단계 7 **Save**(저장)를 클릭합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. [컨피그레이션 변경 사항 구축](#)의 내용을 참조하십시오.


## ID 정책 관리



다중 도메인 구축에서 시스템은 현재 도메인에서 생성된 정책을 표시하며 이러한 정책은 수정할 수 있습니다. 상위 도메인에서 생성된 정책도 표시되지만, 이러한 정책은 수정할 수 없습니다. 하위 도메인에서 생성된 정책을 보고 수정하려면 해당 도메인으로 전환하십시오.


프로시저

단계 1 아직 하지 않았다면 Firepower Management Center에 로그인합니다.

단계 2 **Policies**(정책) > **Access Control**(액세스 제어) > **Identity(ID)** 버튼을 클릭합니다.

단계 3 정책을 삭제하려면 삭제()를 클릭합니다. 컨트롤이 흐리게 표시되는 경우에는 컨피그레이션이 상위 도메인에 속하거나 컨피그레이션을 수정할 권한이 없는 것입니다.

단계 4 정책을 편집하려면 정책 옆에 있는 수정()을 클릭하고 **ID 정책 생성**, 6 페이지에 설명된 대로 변경합니다. 보기()이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

단계 5 정책을 복사하려면 복사()을 클릭합니다.

단계 6 정책에 대한 보고서를 생성하려면 **현재 정책 보고서 생성**에 설명된 대로 보고서()을 클릭합니다.

단계 7 정책을 비교하려면 **정책 비교** 섹션을 참조하십시오.