FMC를 사용하여 수동 ID 에이전트 구성

목차

소개

이 문서에서는 세션 데이터를 FMC에 전송하는 패시브 ID 에이전트 소스를 구성하는 방법에 대해 설명합니다

사전 요구 사항

요구 사항

- 버전 7.6 이상을 실행하는 Cisco Secure Firewall Management Center
- 버전 7.6 이상을 실행하는 Cisco Secure Firewall
- Windows Active Directory 서버에서는 Windows Server 2008 이상을 실행해야 합니다.
- Secure Firewall Threat Defense 디바이스에서 Snort 3을 활성화해야 합니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco Secure Firewall Management Center 7.6.5
- Cisco 보안 방화벽 7.6.5
- Windows Server 2022에서 실행되는 Microsoft Active Directory.

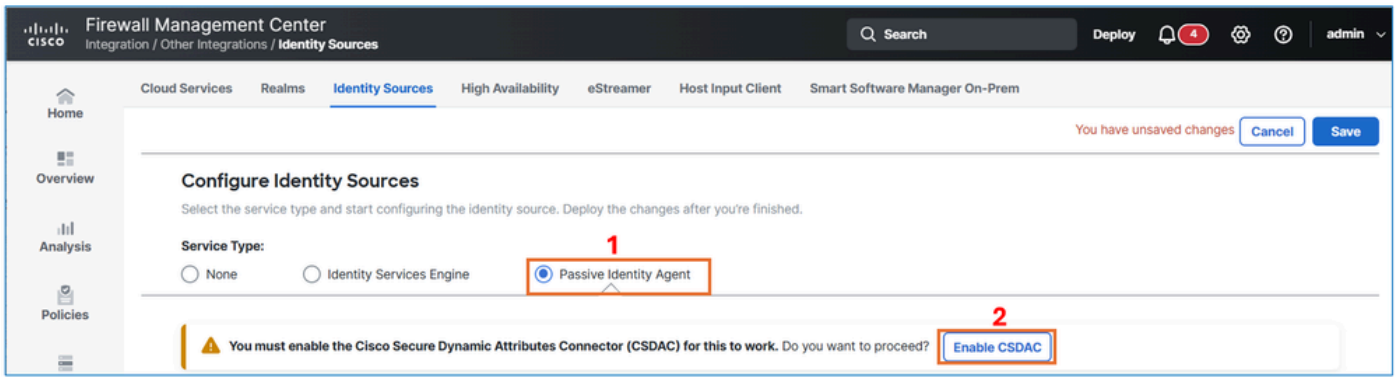
이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

설정

에이전트를 구성하기 전에 AD 및 FMC 통합을 완료하십시오.

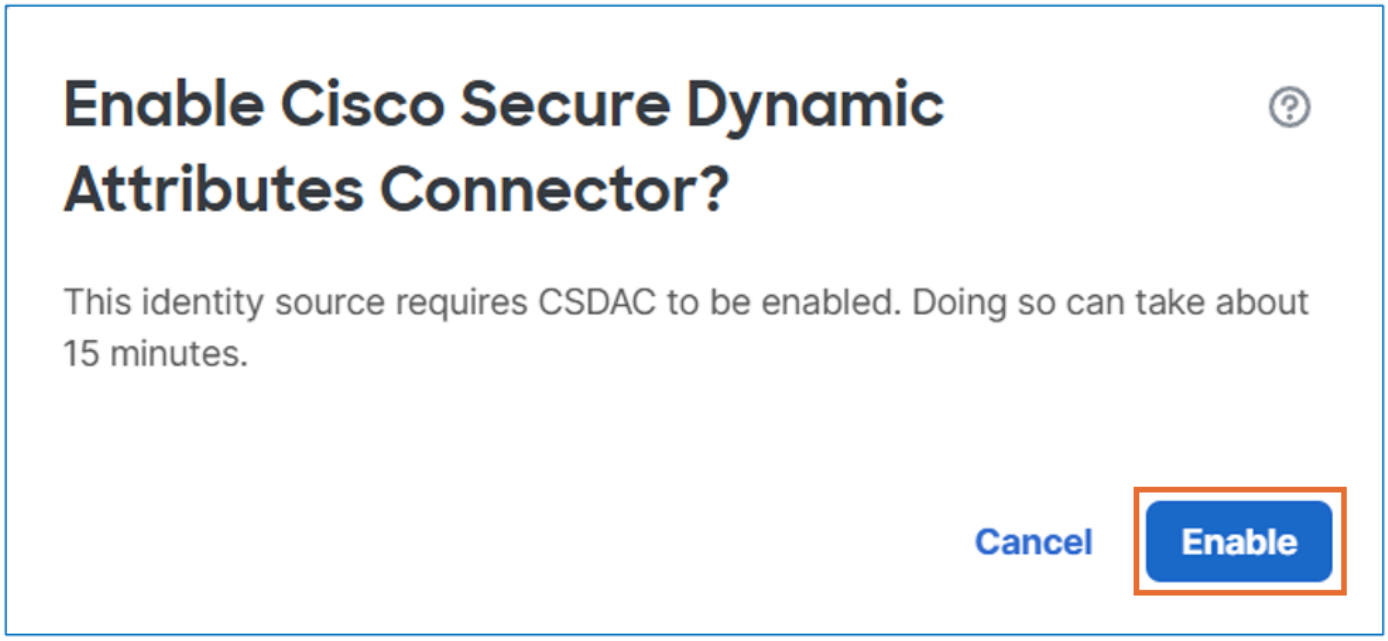
수동 ID 에이전트 소스 구성

FMC UI에서 Integration(통합) > Other Integrations(기타 통합) > Identity Sources(ID 소스)로 이동하고 Passive Identity Agent(수동 ID 에이전트)를 클릭합니다. Cisco Secure Dynamic Attributes Connector가 아직 활성화되지 않은 경우 Enable CSDAC(CSDAC 활성화)를 클릭하여 활성화하라는 메시지가 표시됩니다.



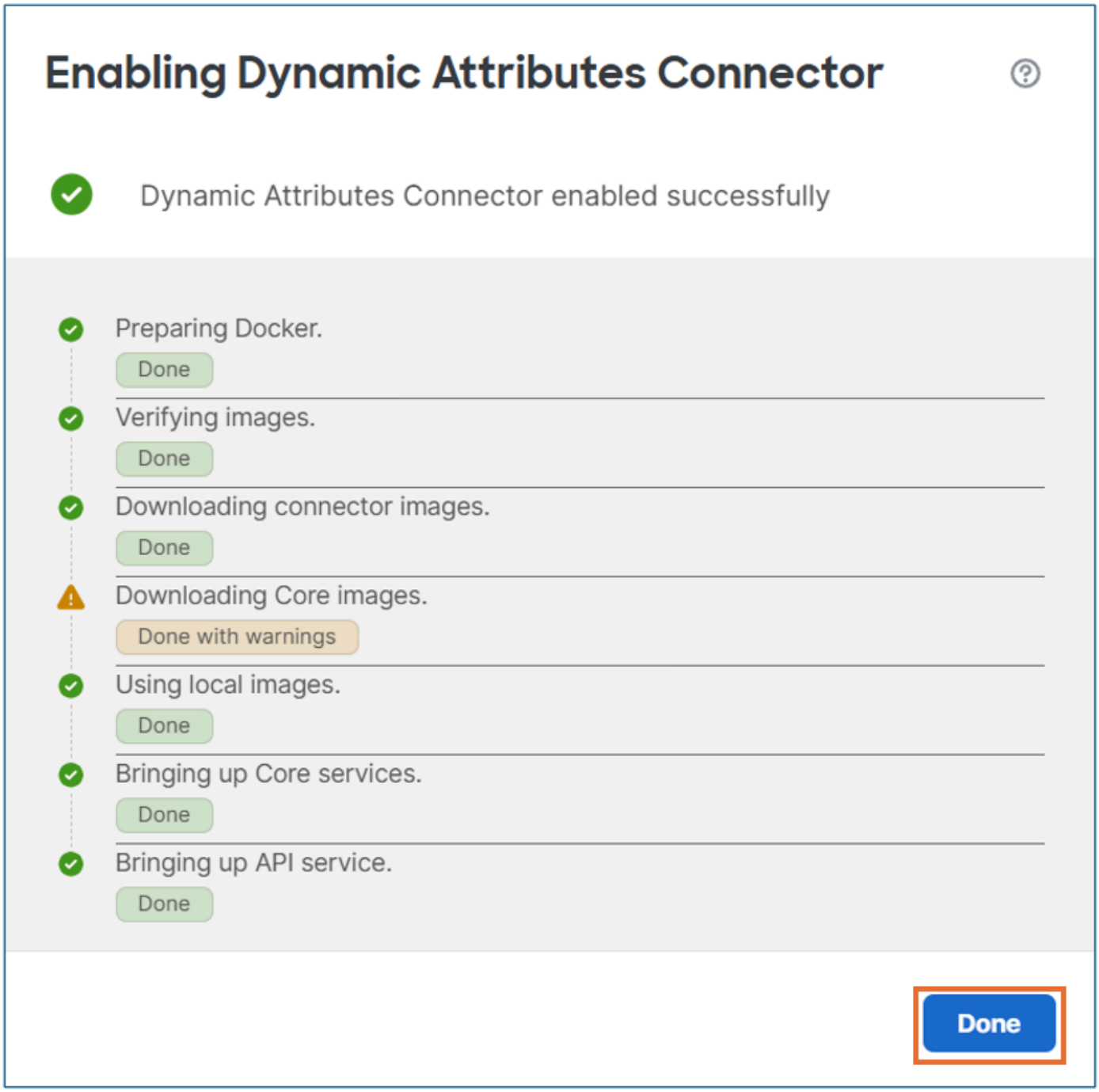
수동 ID 에이전트

Enable(활성화) 버튼을 클릭하여 CSDAC를 활성화합니다.



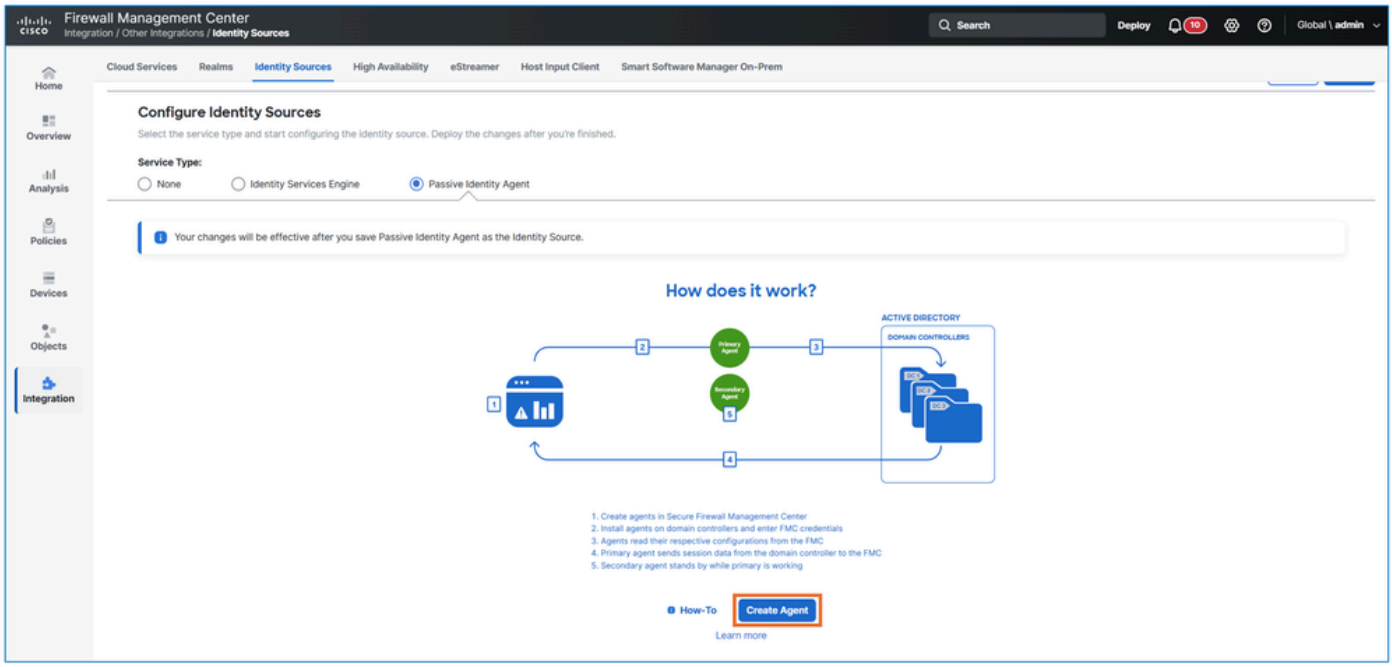
CSDAC 사용

이 단계는 약 10분 정도 소요됩니다. CSDAC가 제대로 활성화되면 Donebutton을 클릭하여 계속 진행합니다.



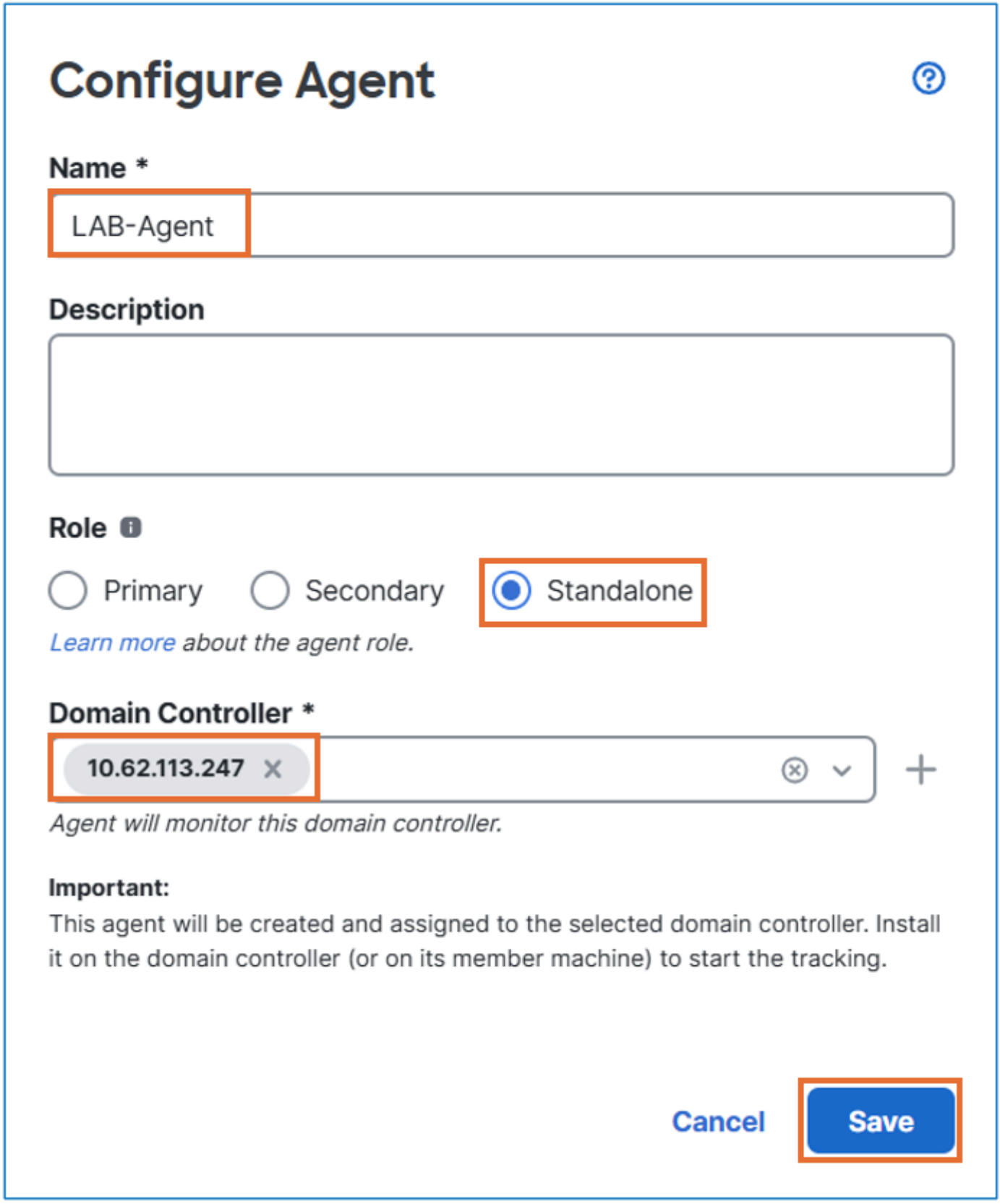
CSDAC 사용

에이전트 생성 단추를 누릅니다.



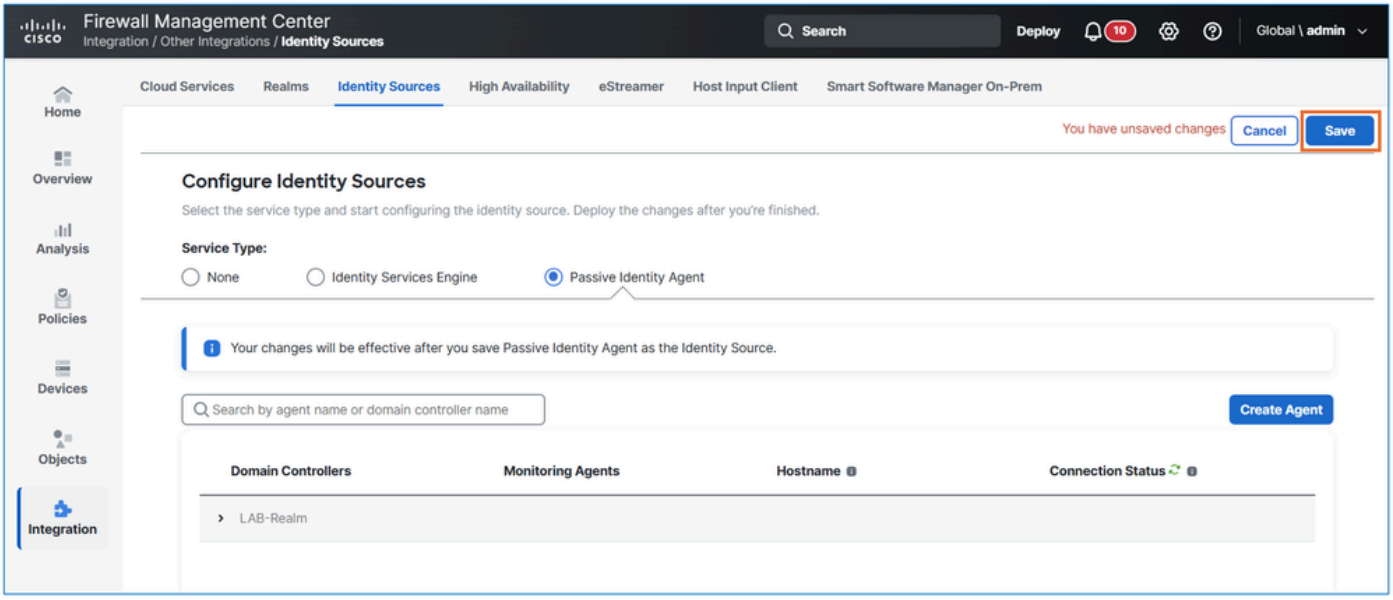
에이전트 생성

상담원의 이름을 정의하고 Standaloneoption을 선택한 다음 이전 작업에서 만든 해당 Domain Controller와 연결합니다.



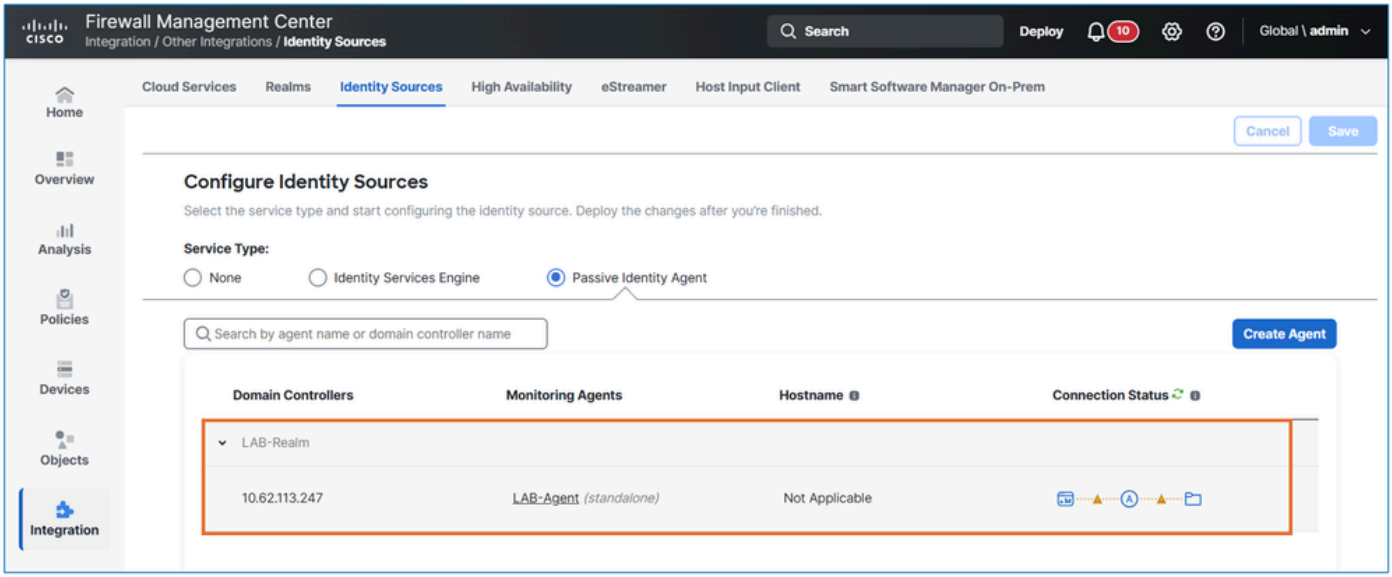
에이전트 구성

저장 버튼을 클릭합니다.



설정 저장

결과.



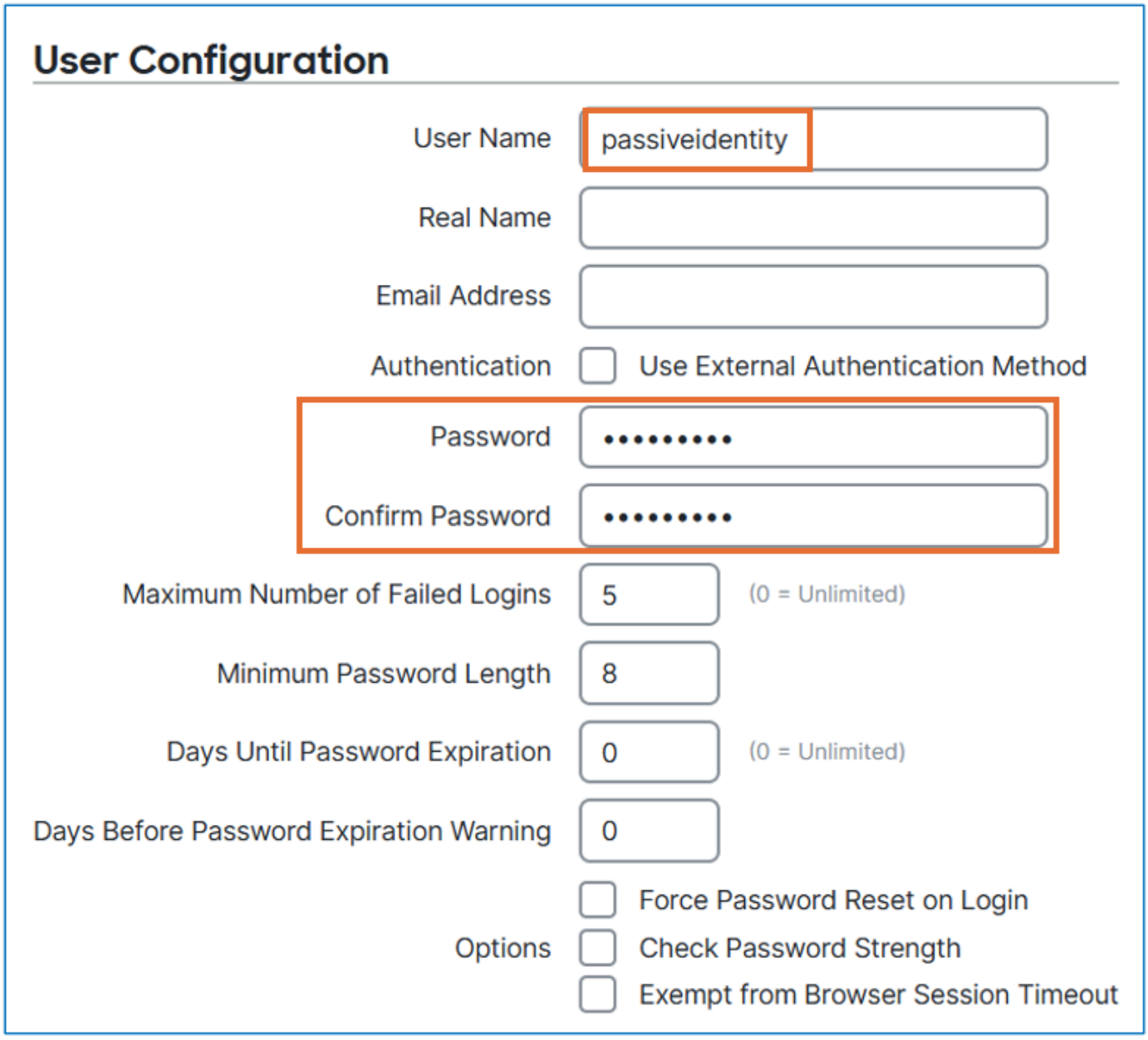
상태 확인

참고: 패시브 ID 에이전트는 회선을 사용하여 상태를 나타내고, 주황색은 에이전트가 Secure Firewall Management Center와 성공적으로 통신한 적이 없음을 의미합니다. 새로 생성된 에이전트 행은 주황색이며 컨피그레이션이 완료될 때까지 유지됩니다.

Secure Firewall Management Center에서 수동 ID 에이전트 사용자 생성

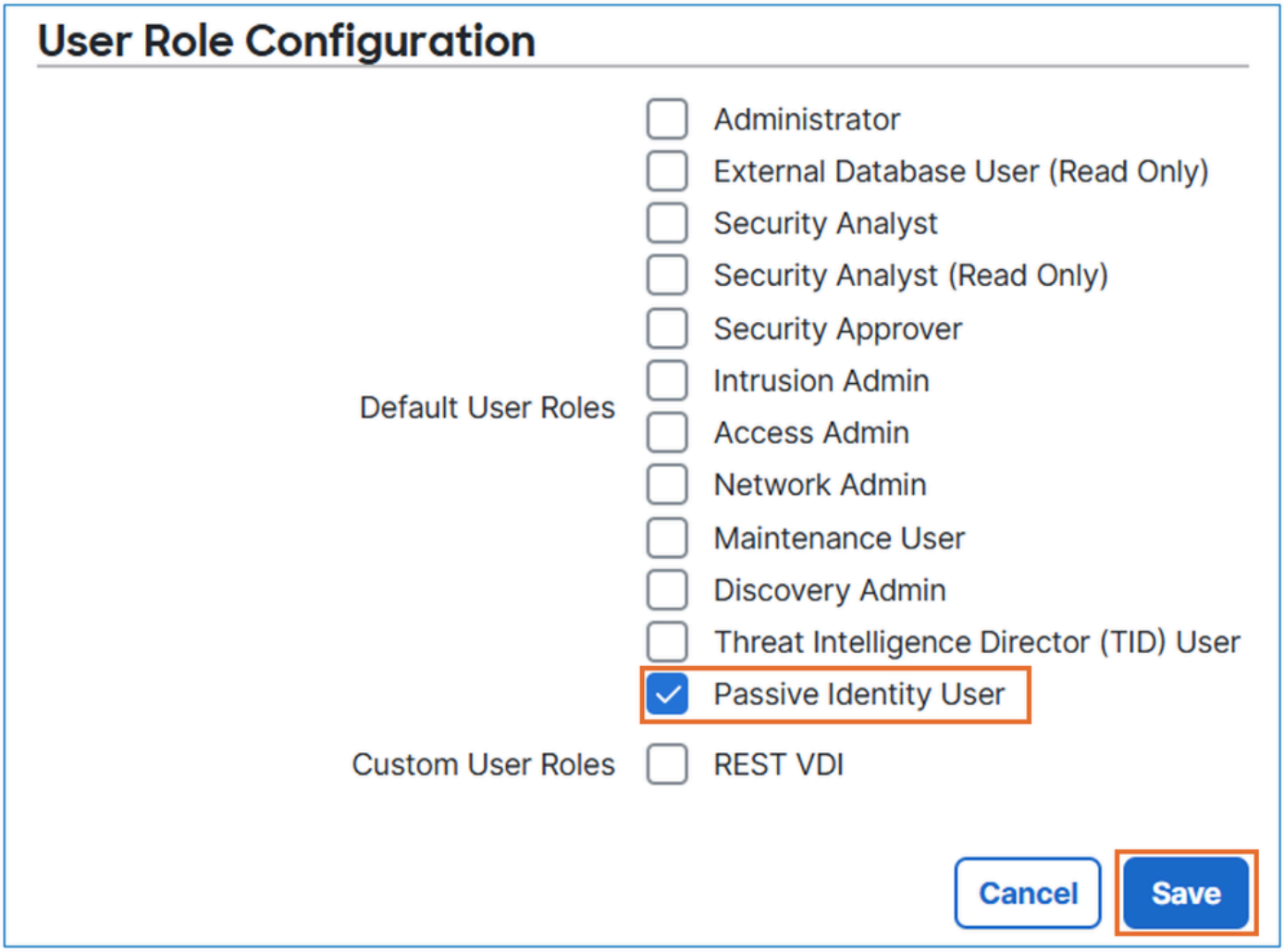
수동 ID 에이전트와 통신할 수 있는 권한이 있는 Secure Firewall Management Center 사용자를 만듭니다. 이 사용자는 다른 작업을 수행할 수 있는 제한된 권한을 가집니다. 사용자는 패시브 id 에이전트와의 통신만 활성화해야 합니다.

FMC UI에서 System(시스템) > Users(사용자)로 이동하고 Create User(사용자 생성)를 클릭합니다. 작업 요구 사항에 따라 사용자 세부 정보를 입력합니다.



사용자 생성

Passive Identity Userrole만 할당합니다. 저장 버튼을 클릭합니다.

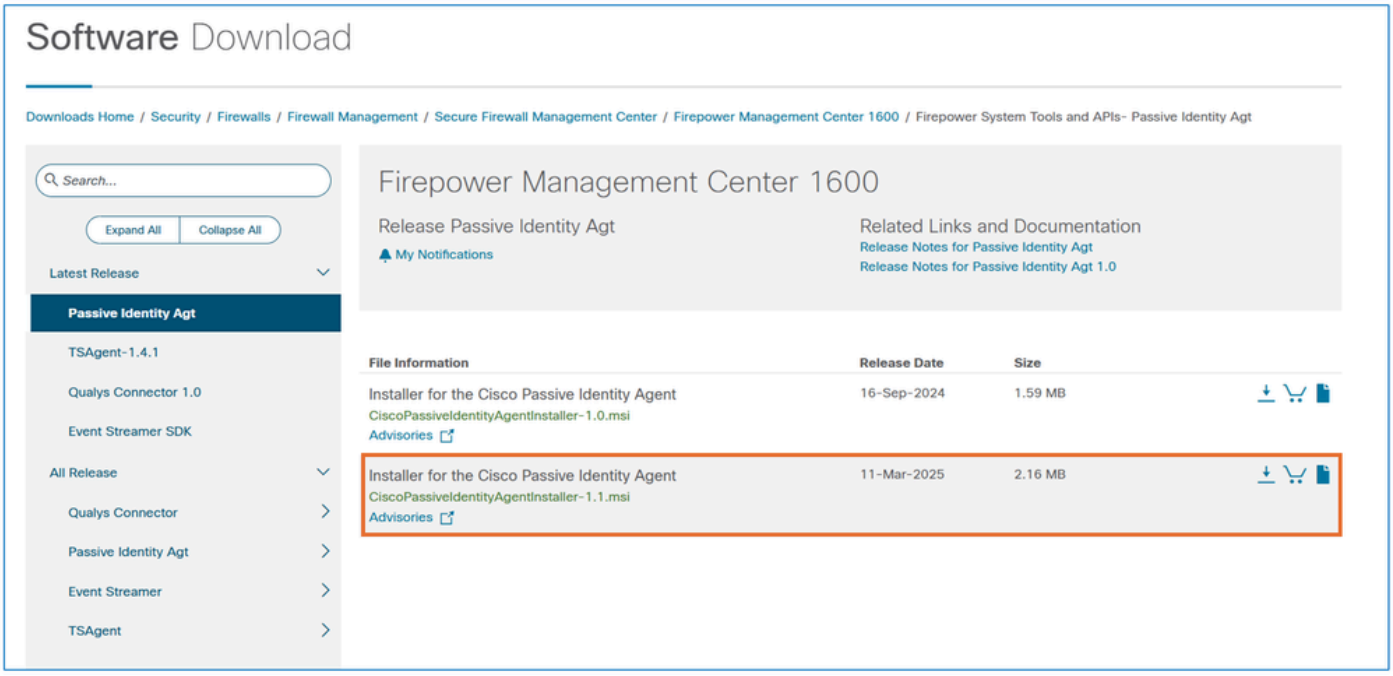


수동 id 사용자 선택

Passive Identity Agent 소프트웨어 설치 및 구성

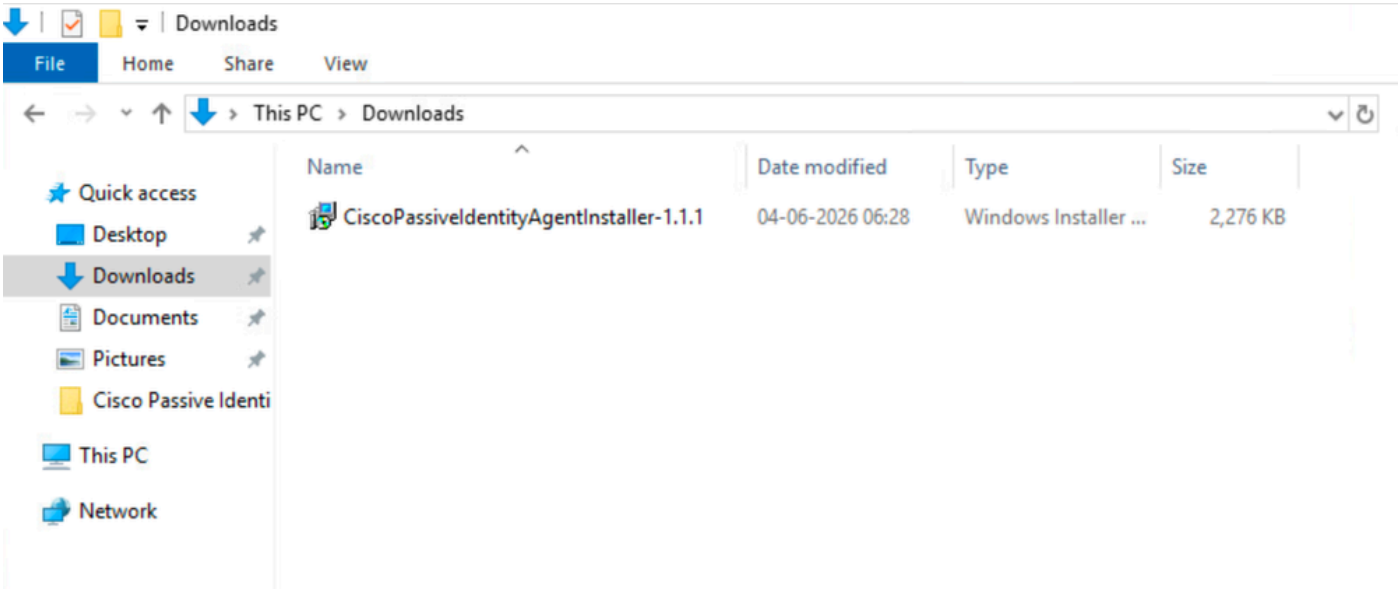
지정된 도메인 컨트롤러에 Passive Identity Agent 소프트웨어를 설치 및 구성합니다.

software.cisco.com에서 패시브 ID 에이전트를 다운로드합니다.



소프트웨어 다운로드

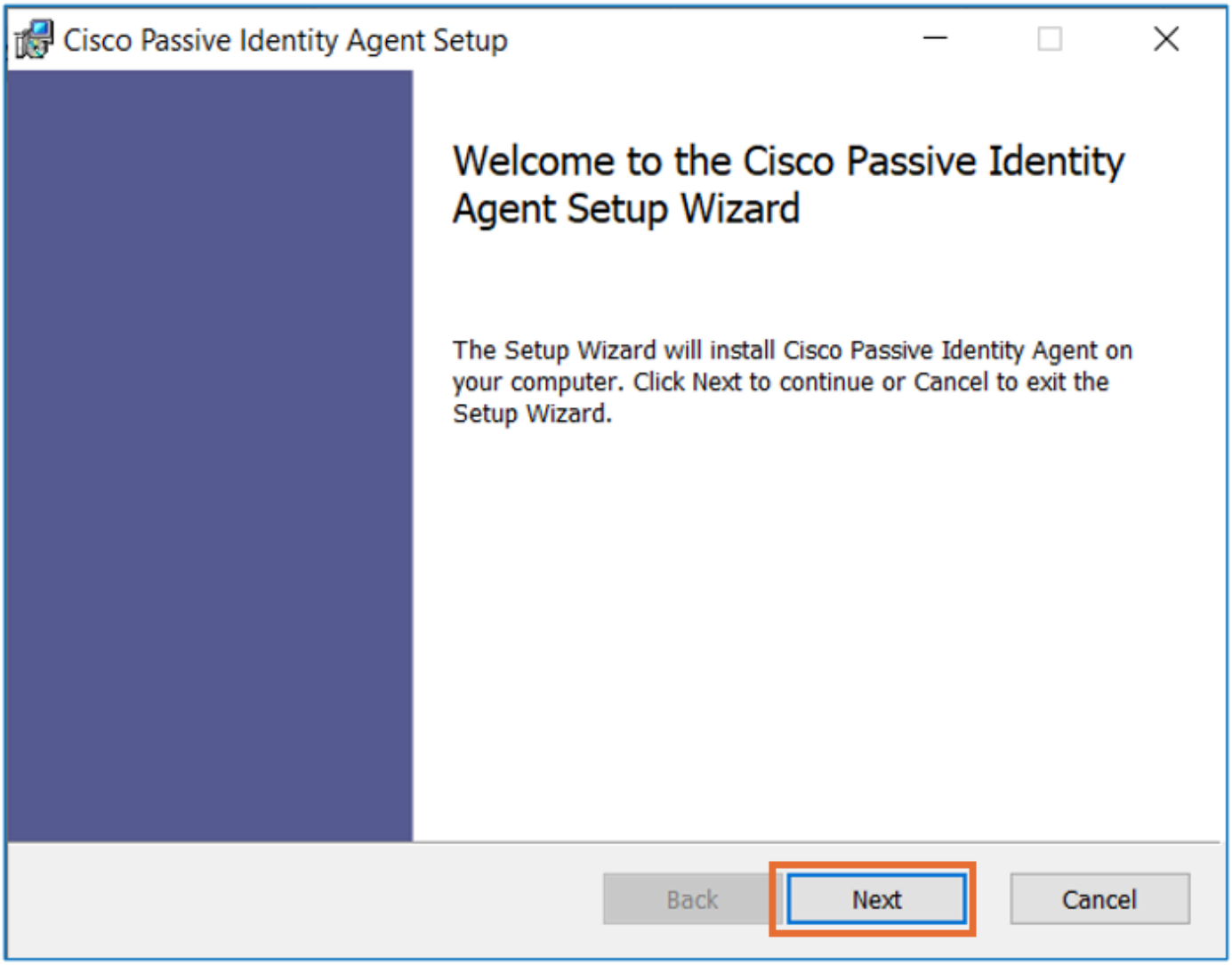
에이전트를 다운로드한 후 도메인 컨트롤러에서 설치 프로세스를 시작합니다.



대리인

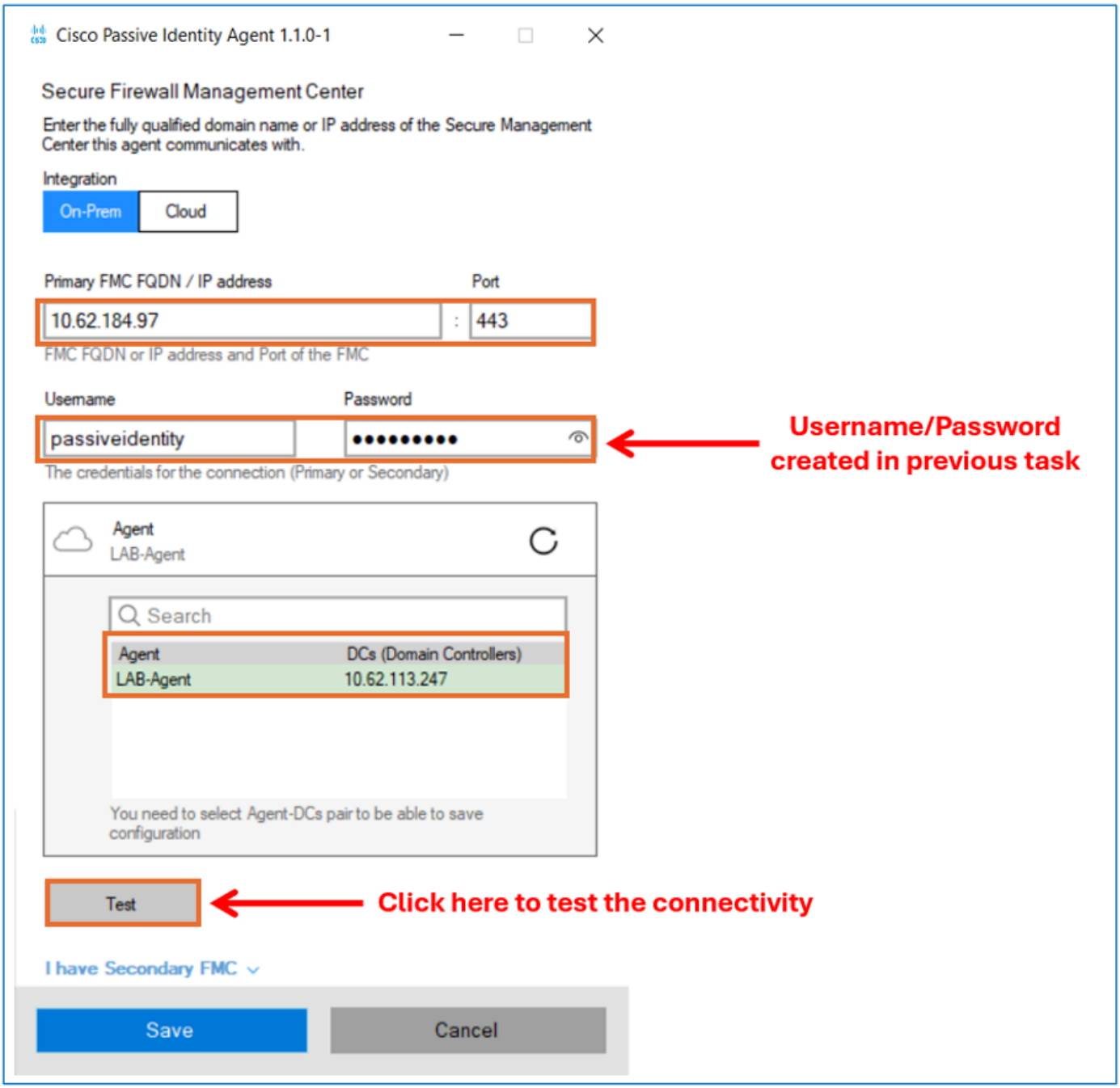
]

제공된 설치 지침을 참조하여 설치를 완료합니다.



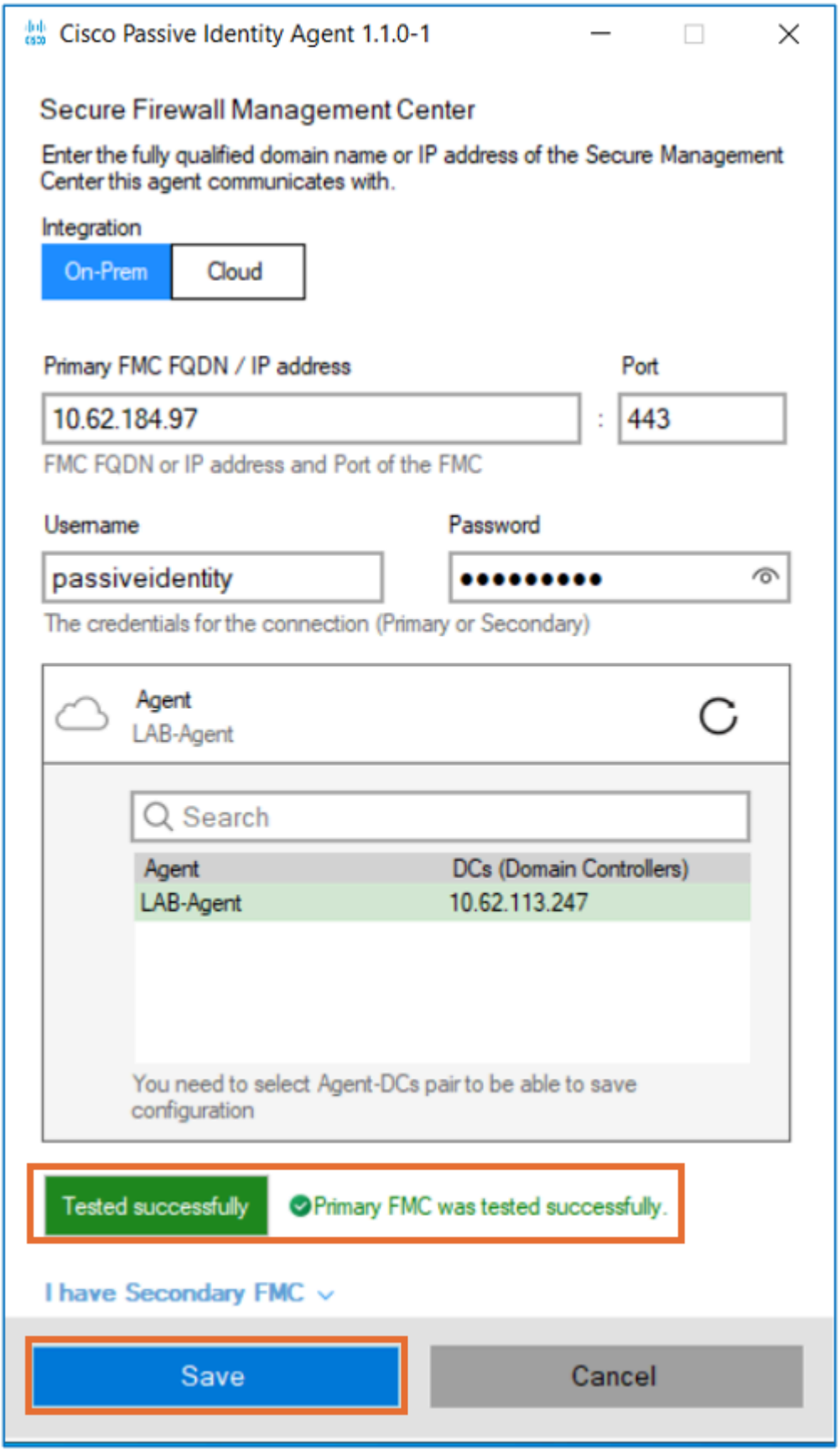
Install

설치가 완료되면 Passive Identity Agent 소프트웨어를 열고 작업 요구 사항에 지정된 대로 필요한 정보를 입력합니다. Test(테스트) 버튼을 클릭하여 FMC와의 연결을 확인합니다.



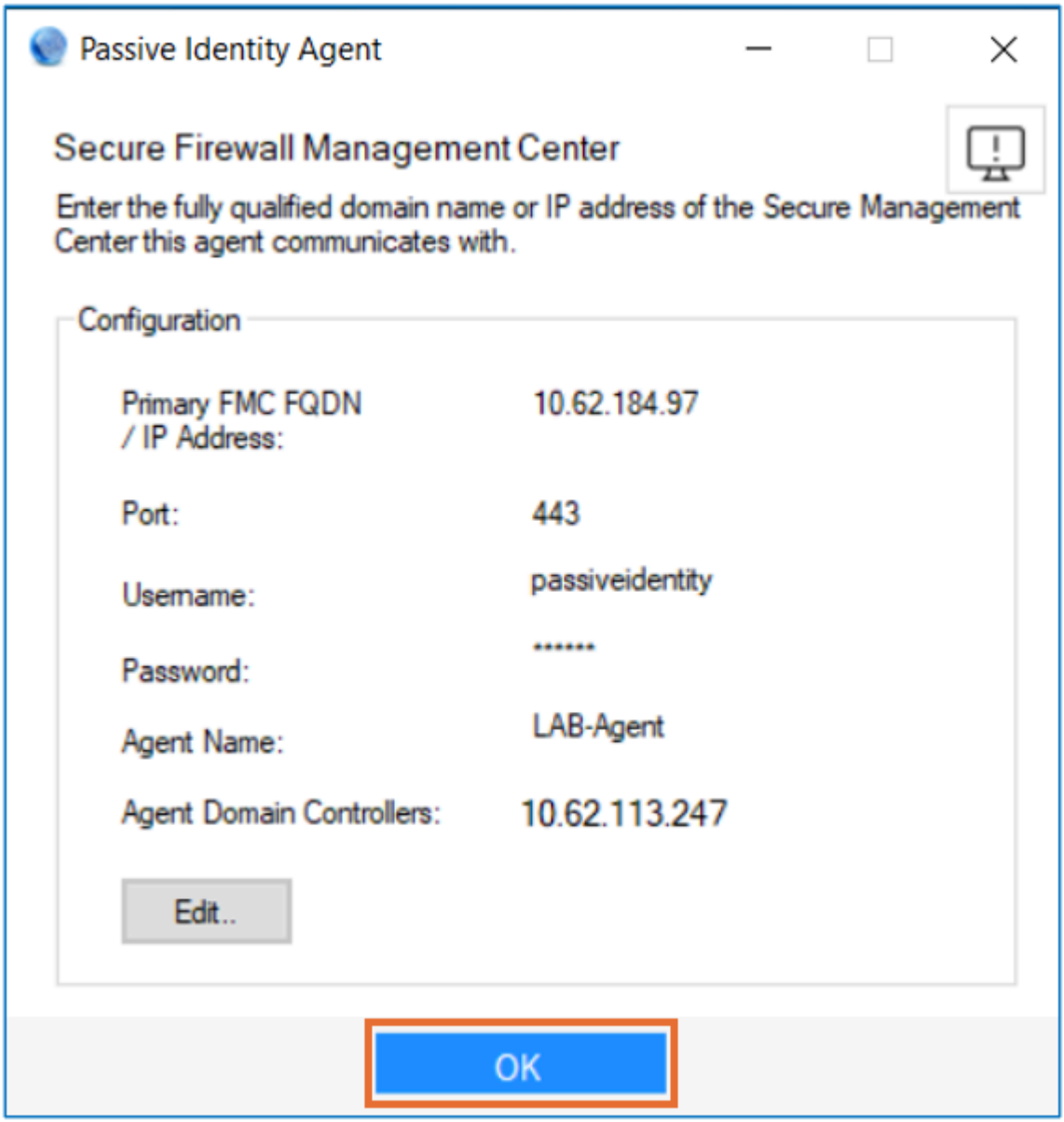
에이전트를 구성합니다.

연결을 성공적으로 테스트한 후 Save(저장) 버튼을 클릭합니다.



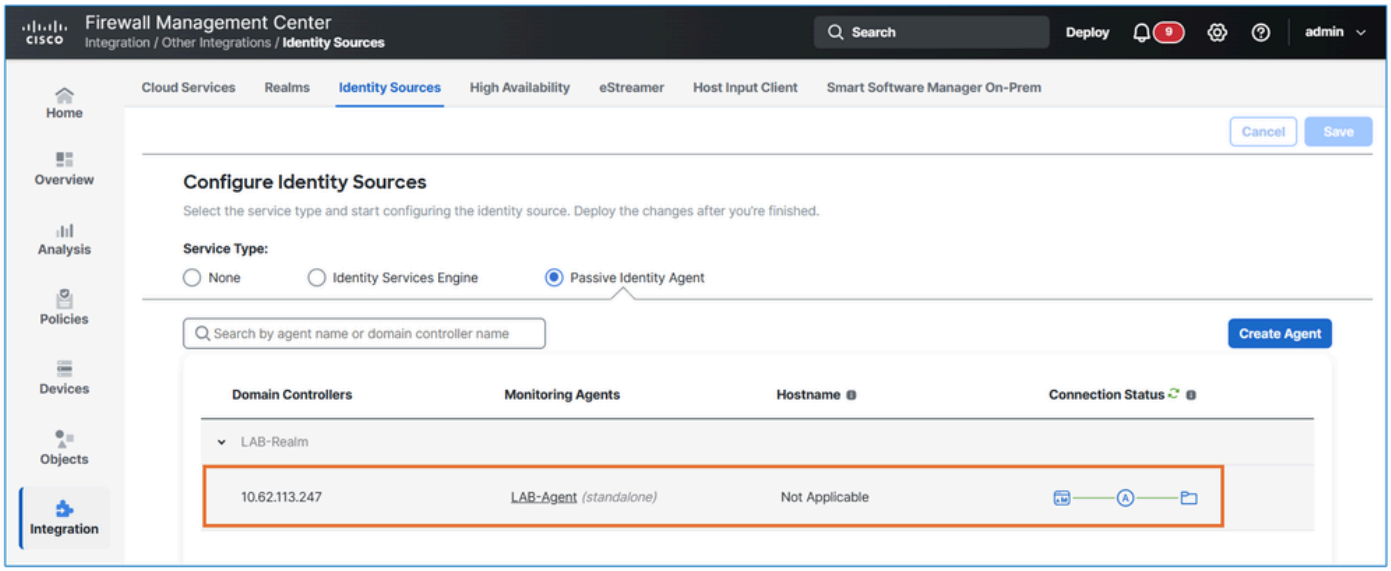
테스트

OK(확인) 버튼을 클릭하여 에이전트 컨피그레이션을 완료합니다.



에이전트가 실행 중입니다.

FMC UI에서 Integration(통합) > Other Integrations(기타 통합) > Identity Sources(ID 소스) > Passive Identity Agent로 이동합니다. Passive Identity Agent가 녹색 상태를 표시하는지 확인합니다.



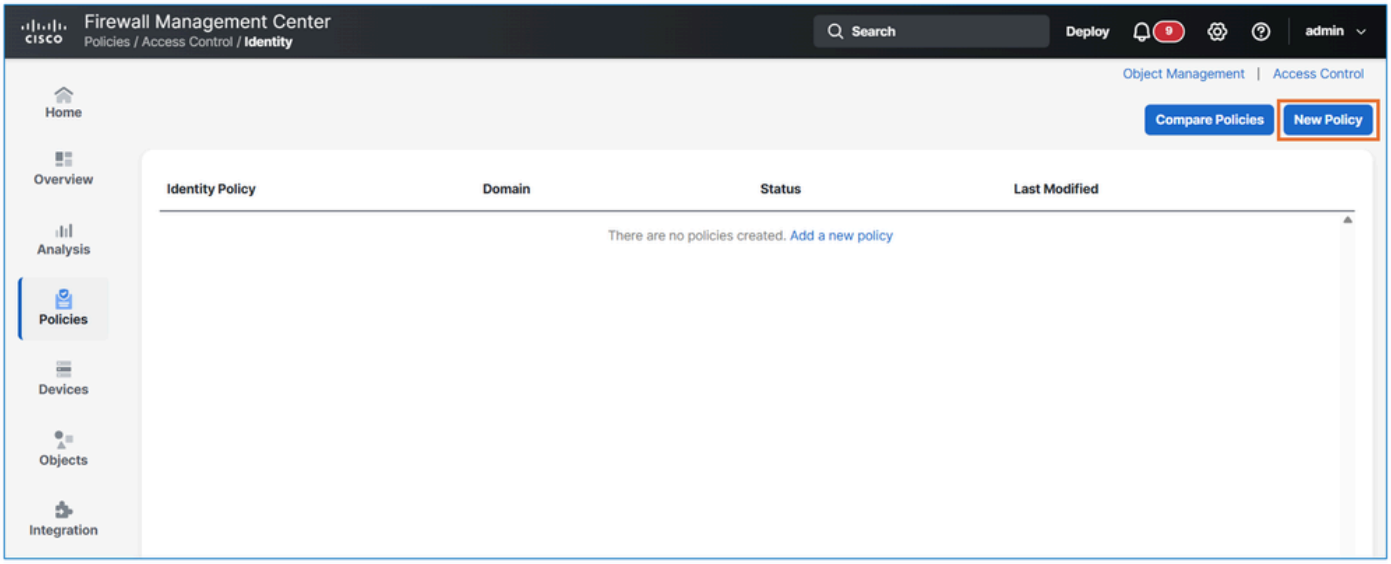
fmc의 통신 확인

ID 정책 구성

제공된 테이블을 기반으로 ID 정책을 생성합니다.

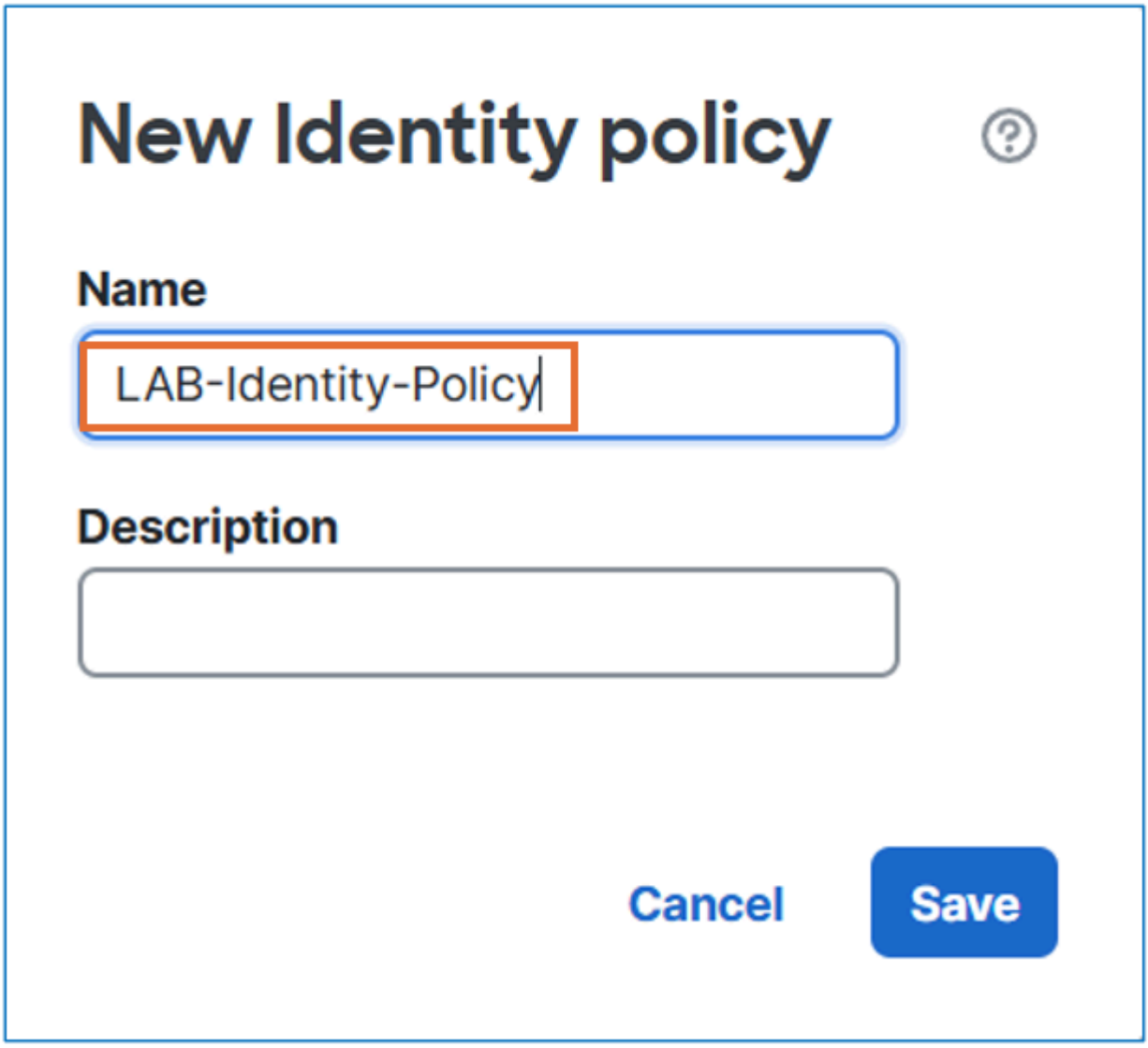
정책 이름	규칙 이름	인증 영역	나머지 설정
랩 ID 정책	규칙1	실습 영역	기본값으로 유지

FMC UI에서 Policies(정책) > Access Control(액세스 제어) > Identity(ID)로 이동합니다. 새 정책 단추를 클릭합니다.



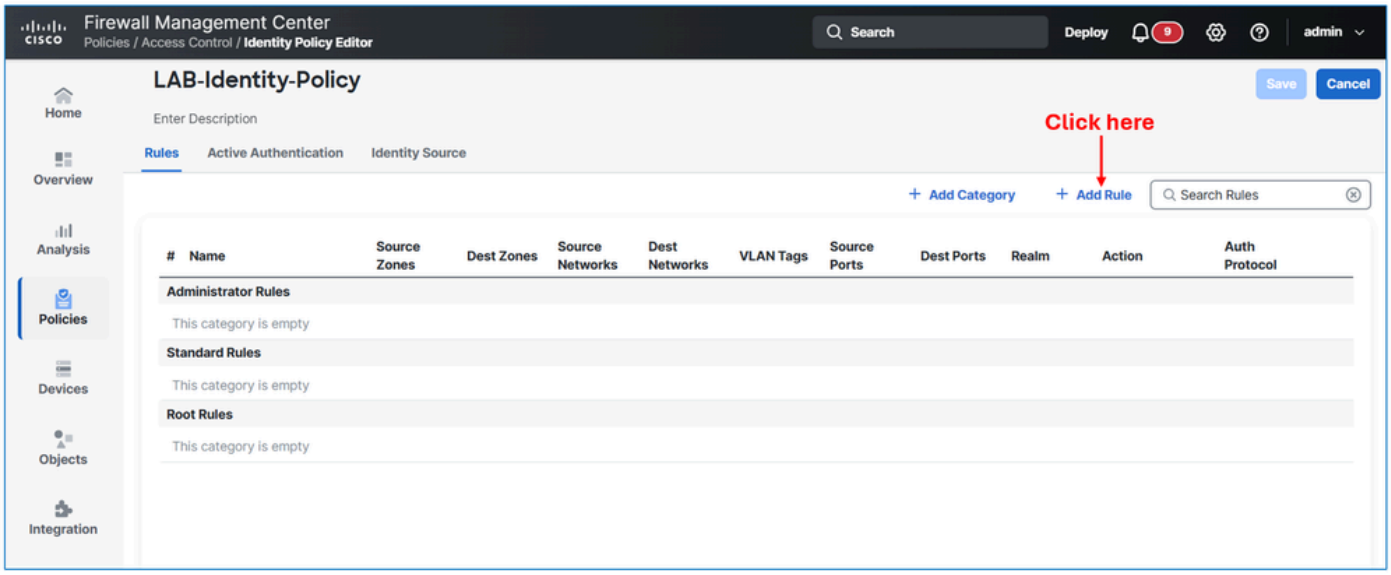
새 정책

작업 요구 사항에 따라 정책 이름을 입력합니다.



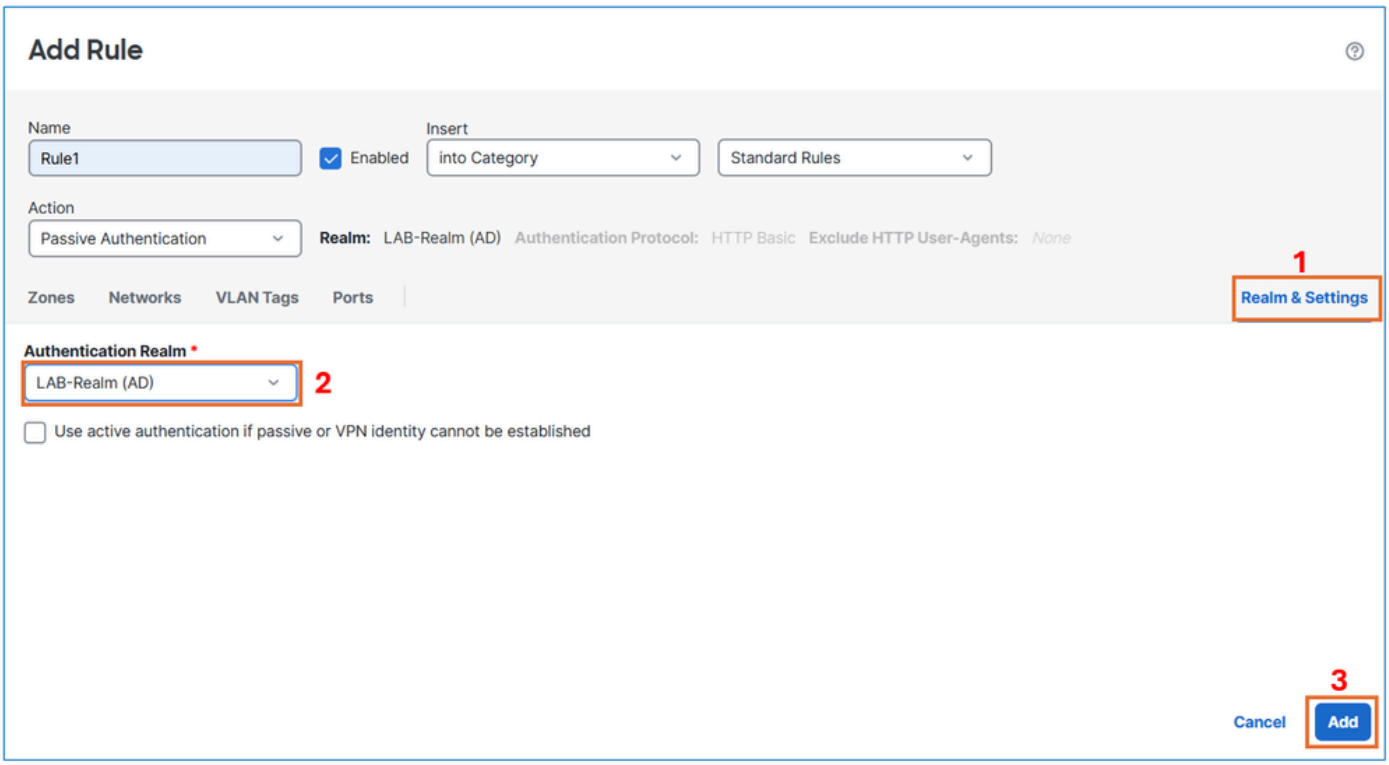
새 정책

규칙 추가 단추를 클릭합니다.



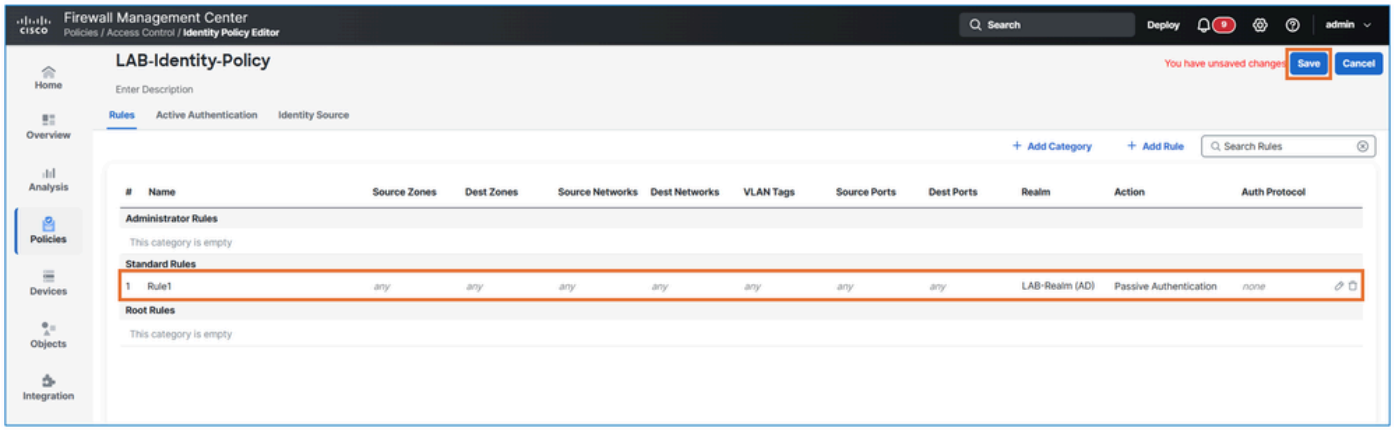
규칙 만들기

Realm & Settings(영역 및 설정) 탭으로 이동하고 작업 요구 사항에 따라 Authentication Realbed(인증 영역)를 선택합니다. 마지막으로 Addbutton을 클릭합니다.



영역 설정

저장 버튼을 클릭합니다.



컨피그레이션 저장

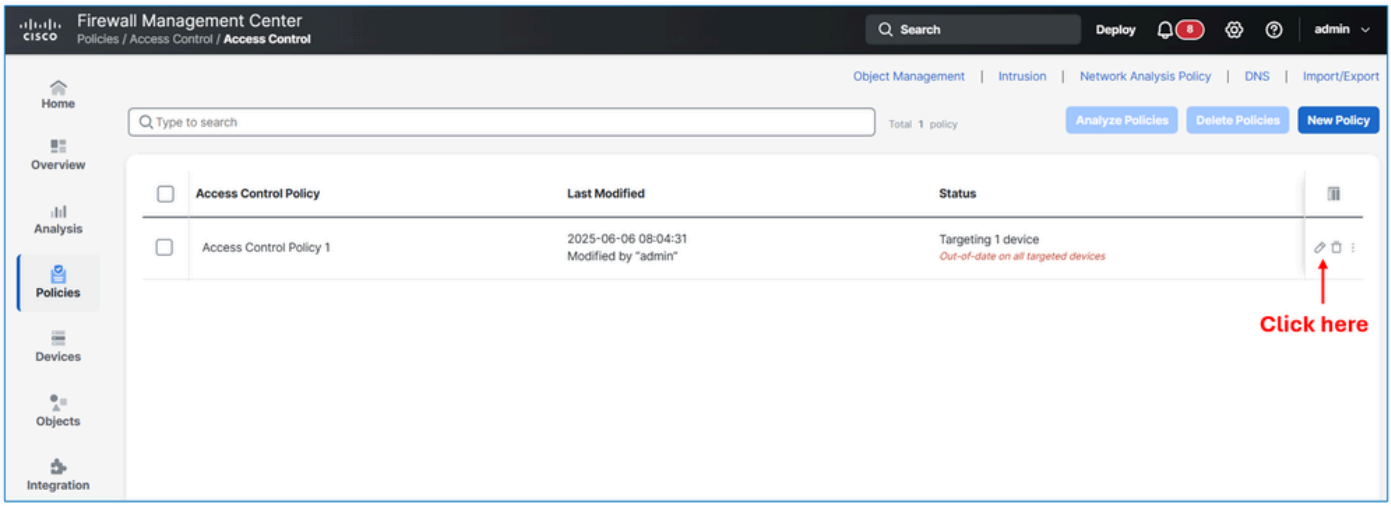
액세스 제어 정책 구성

ID 정책을 액세스 제어 정책에 연결하고 다음과 같은 특성으로 액세스 정책 규칙을 생성합니다.

속성 이름	가치
규칙 이름	규칙1
작업	허용
소스 영역	내부
대상 영역	외부
소스 네트워크	10.10.10.0/24
대상 네트워크	10.48.62.98/32
서비스	대상 포트 TCP 80(HTTP)
사용자	LAB-영역/그룹1
로깅	연결 종료 시

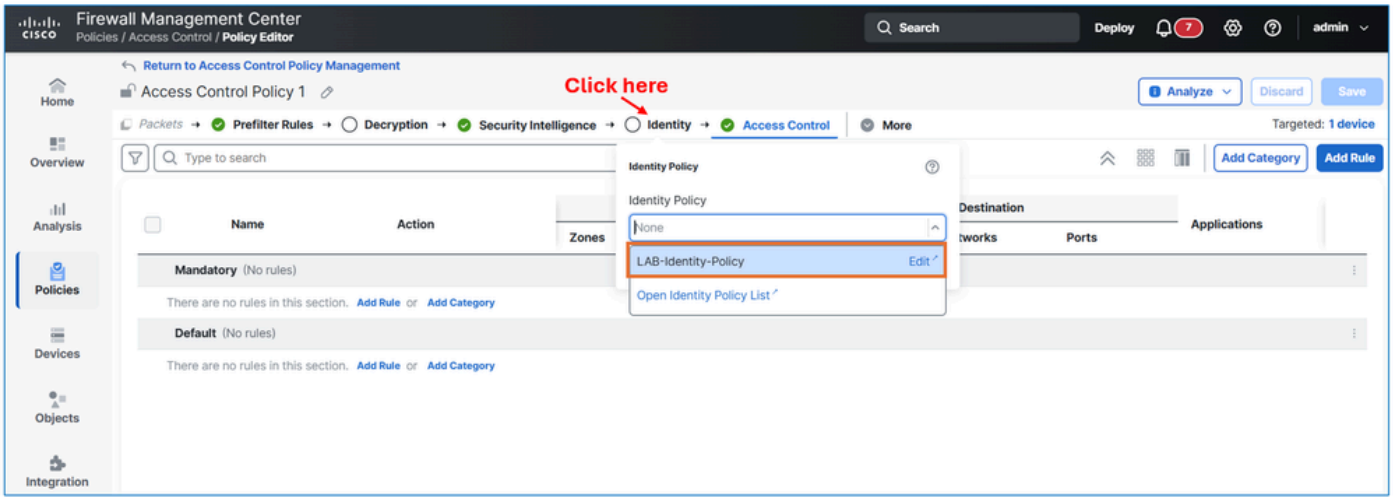
1단계. ID 정책을 액세스 제어 정책에 연결

FMC UI에서 Policies(정책) > Access Control(액세스 제어) > Access Control(액세스 제어)로 이동합니다. 정책에 대한 편집 단추를 클릭합니다.



정책 편집

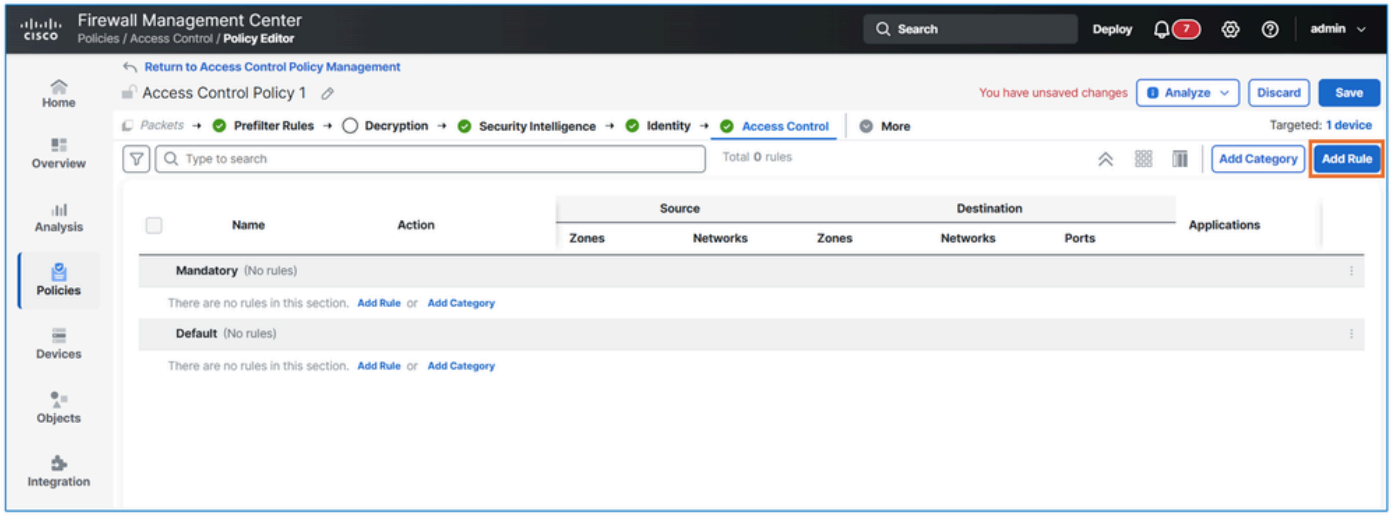
Identitysection으로 이동하여 이전 작업에서 생성한 ID 정책을 연결합니다.



id 정책 추가

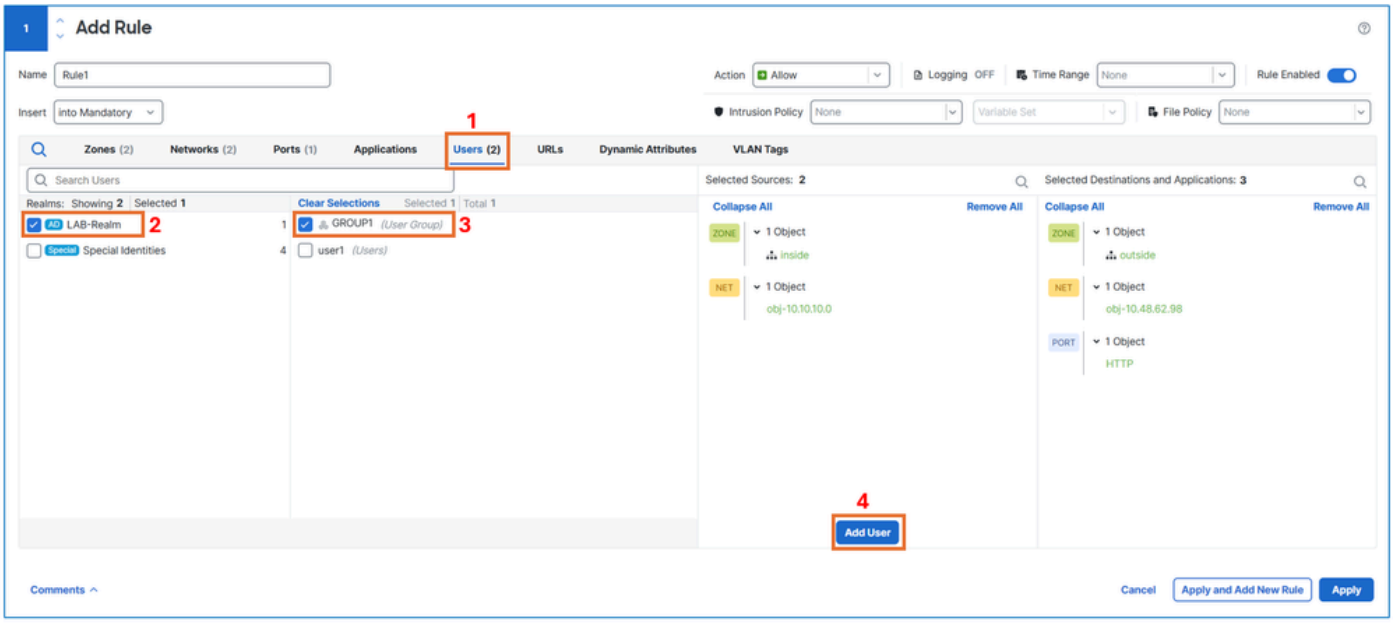
Applybutton을 클릭합니다

2단계. 액세스 제어 규칙을 생성합니다.



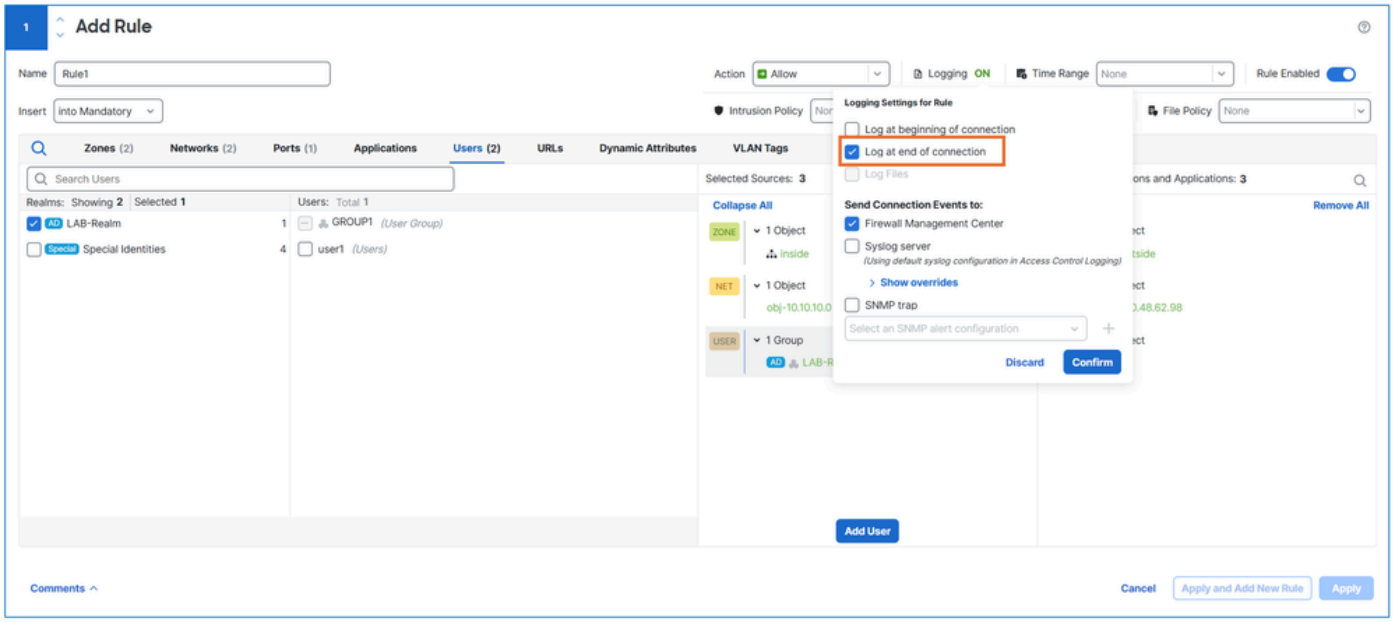
ACP 생성

작업 요구 사항에 따라 세부 정보를 입력합니다. 가장 중요한 것은 사용자 탭 아래에 addGROUP1 fromLAB-Realm을 입력합니다.



규칙에 사용자 추가

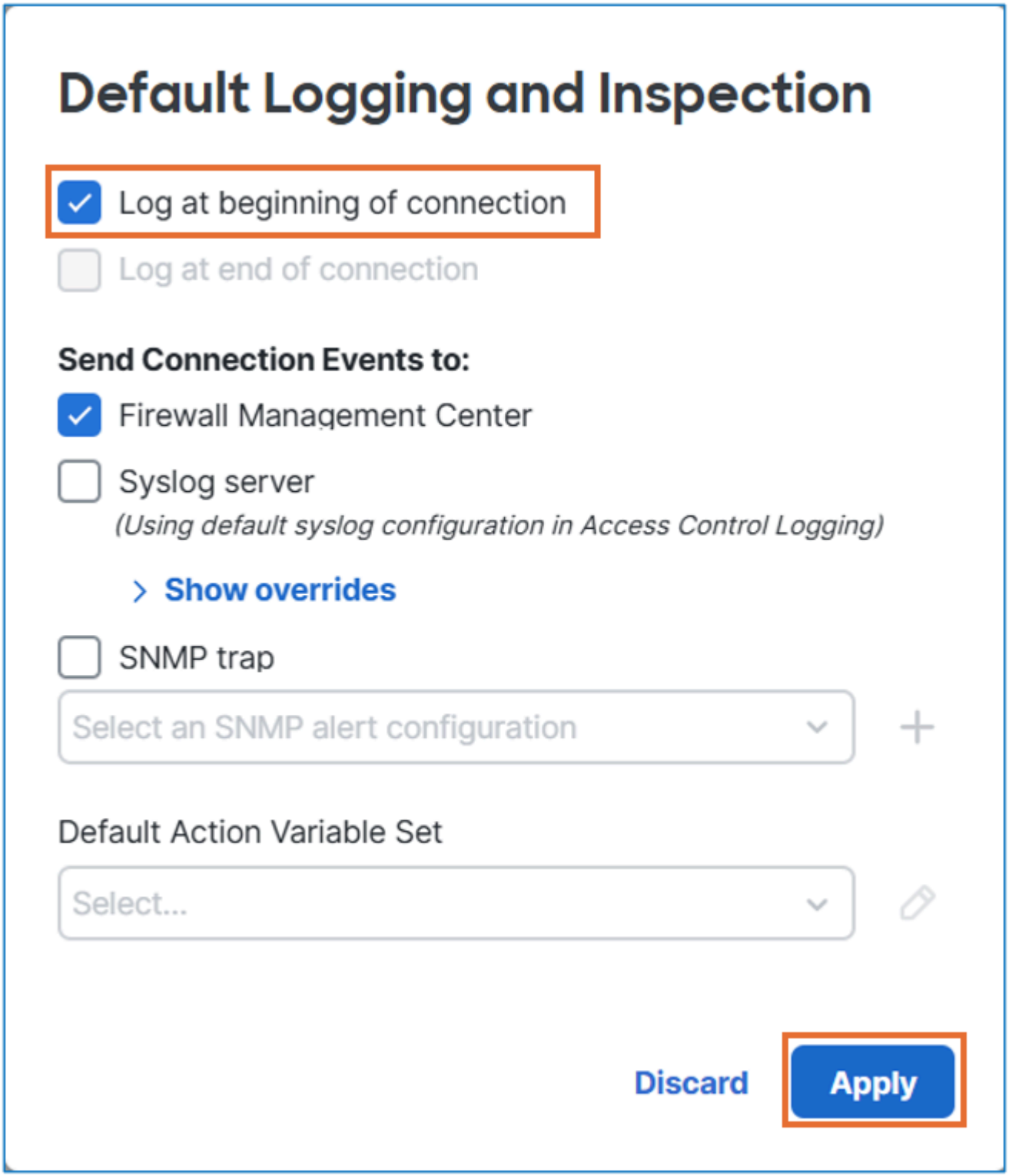
Log at end of connection(연결 종료 시 로그)을 선택하여 규칙에 대한 로깅을 활성화합니다.



로깅 사용

3단계. 기본 작업에 대한 로깅을 활성화합니다.

설정아이콘을 눌러 기본 작업 로깅 설정을 수정합니다.



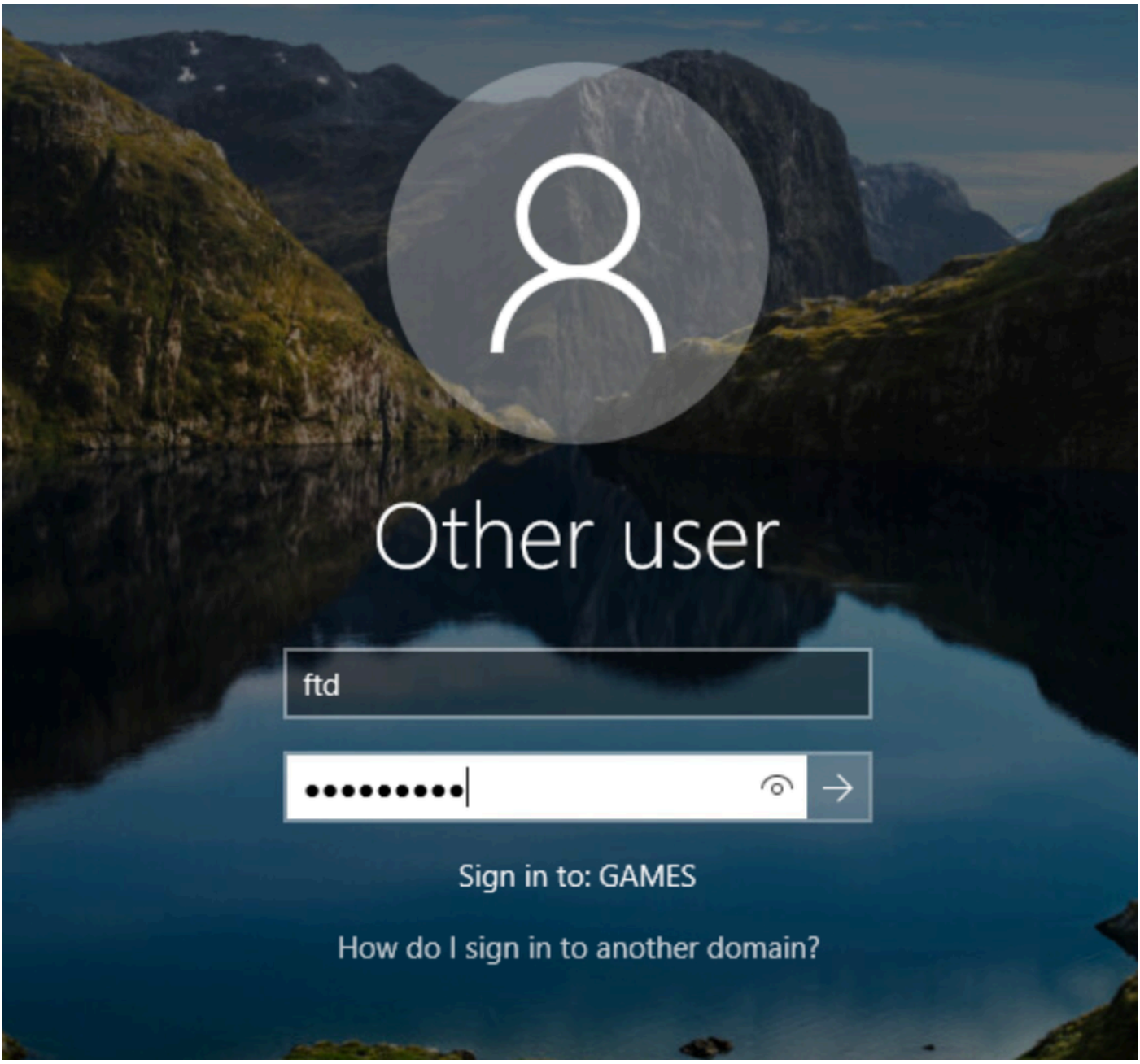
로깅 사용

저장 및 배포FTD에 컨피그레이션을 구축합니다.

확인

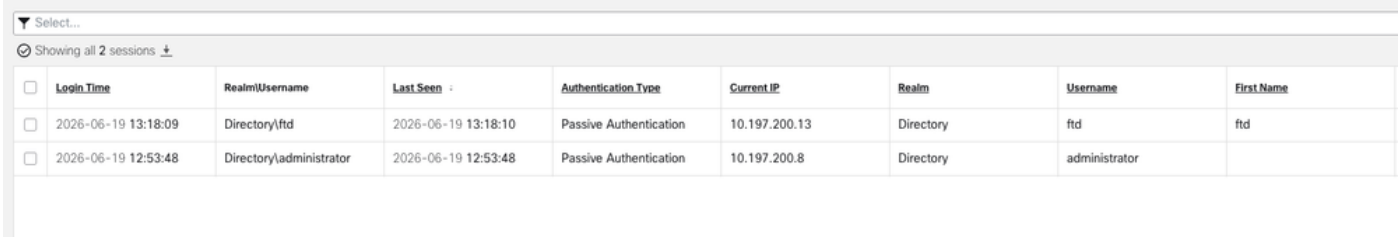
트래픽이 ftd 전용으로 허용되는지 확인하여 Passive Identity 작업을 확인합니다.

사용자 시스템에서 도메인 사용자에 로그인합니다.



사용자 로그인

사용자가 성공적으로 로그인한 후 FMC의 Analysis(분석) > user(사용자) >active session(활성 세션)에서 활성 사용자 세부 정보를 확인합니다.



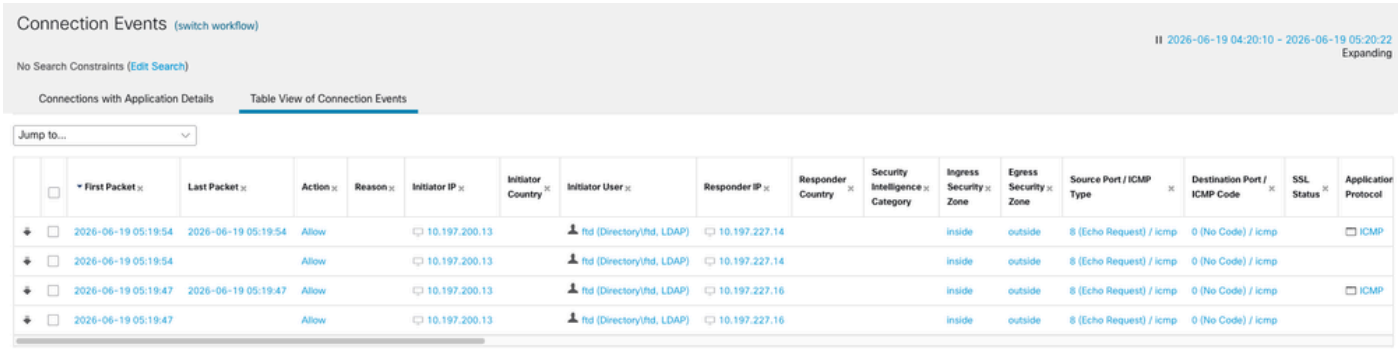
Select...

Showing all 2 sessions

Login Time	Realm\Username	Last Seen	Authentication Type	Current IP	Realm	Username	First Name
2026-06-19 13:18:09	Directory\ftd	2026-06-19 13:18:10	Passive Authentication	10.197.200.13	Directory	ftd	ftd
2026-06-19 12:53:48	Directory\administrator	2026-06-19 12:53:48	Passive Authentication	10.197.200.8	Directory	administrator	

활성 세션

연결 이벤트에서 일부 트래픽 확인을 시작한 후에는 연결 이벤트의 사용자 세부사항을 참조하십시오.

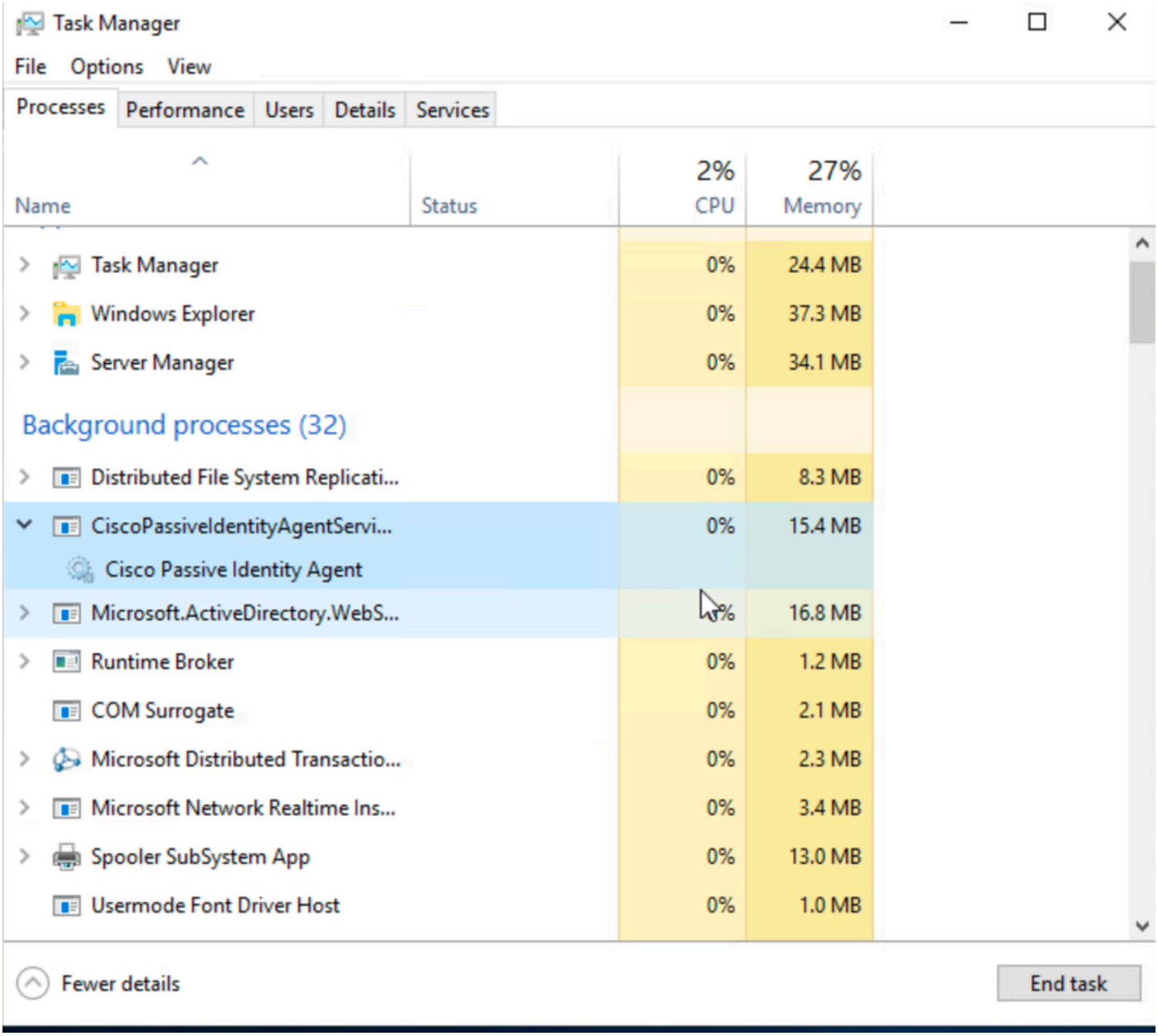


활성 세션

문제 해결

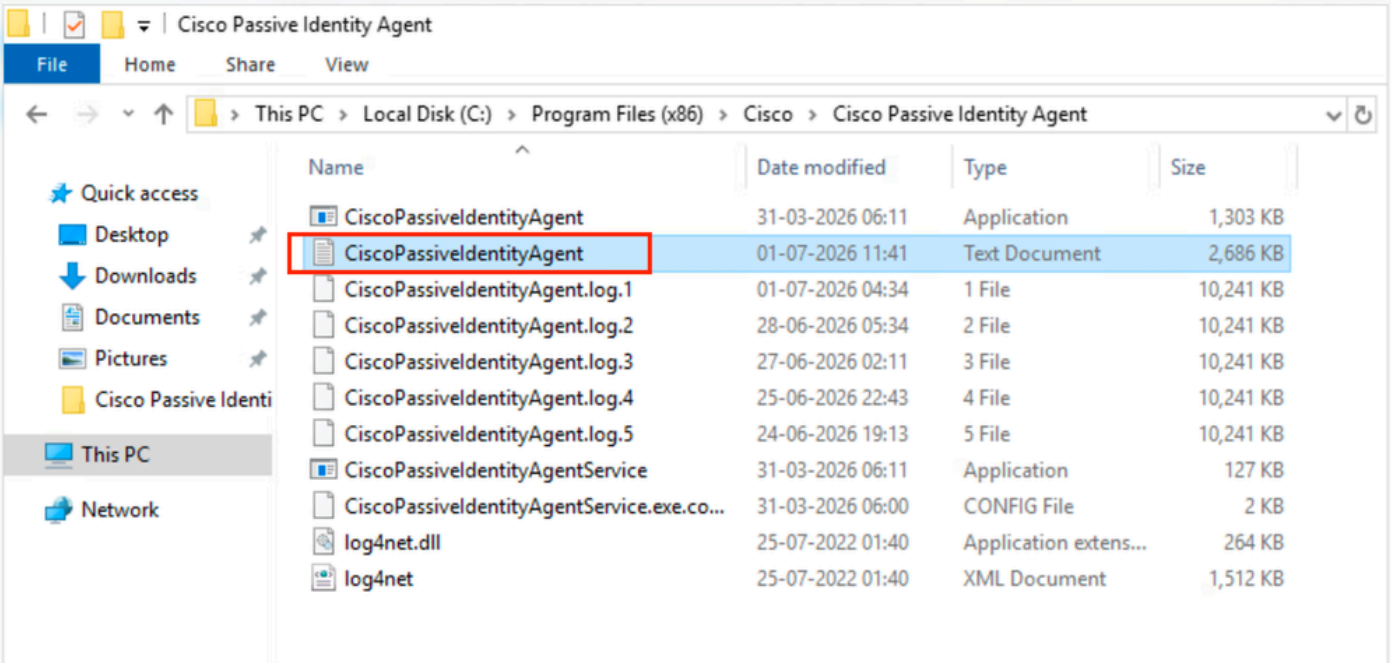
에이전트 로그 확인

에이전트를 호스팅하는 Windows 컴퓨터에서 Task Manager를 열고 백그라운드 프로세스 CiscoPassiveIdentityAgentServices가 실행 중인지 확인합니다.



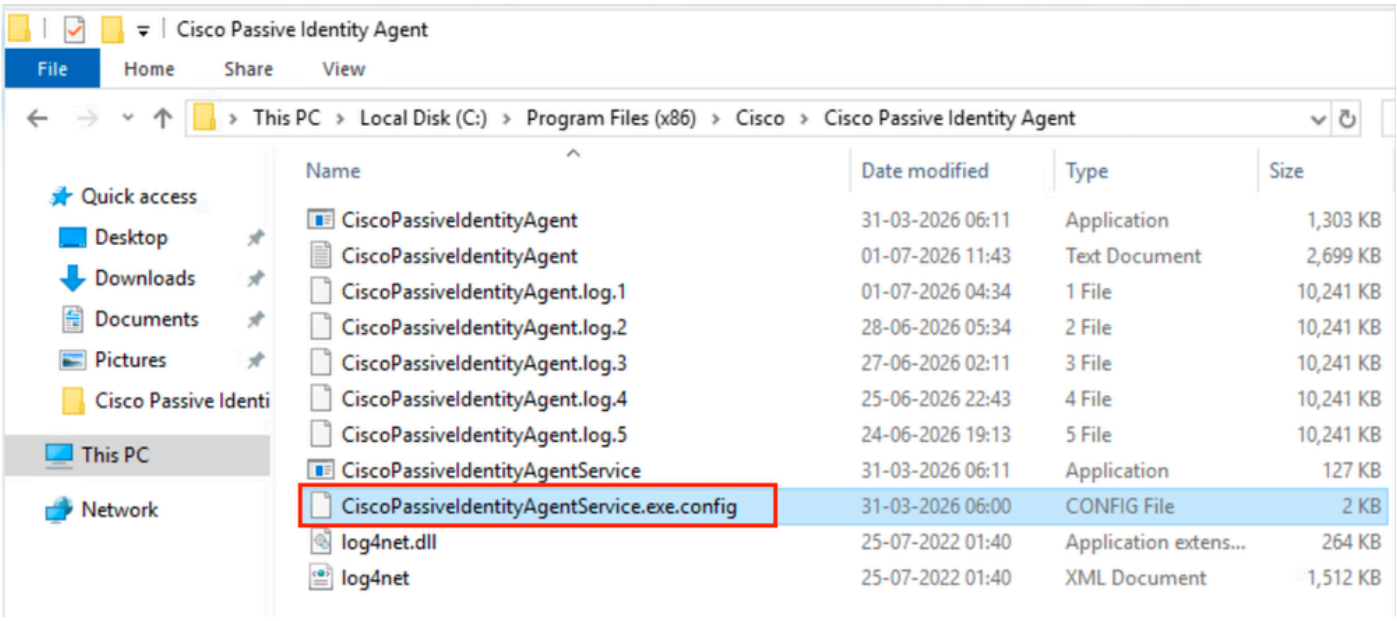
실행 중인 작업

상담원 로그는 CiscoPassiveIdentityAgent 파일에서 찾을 수 있습니다. 기본적으로 위치: "C:\Program 파일(x86)\Cisco\Cisco Passive Identity Agent\"



대리인

기본적으로 에이전트 로그는 INFOlevel로 설정됩니다. DEBUG 레벨 로깅을 활성화하려면 CiscoPassiveIdentityAgentService.exe.configfile을 수정하고 로깅 레벨을 ALLorDEBUG로 설정합니다.



에이전트 구성

정보 로그

에이전트 로그 확인 - 에이전트 컨피그레이션 가져오기

INFO Rest 클라이언트, 대량 이벤트: [f"domain":"games.cisco.com", "srcIpAddress": "X.X.X", "사용자": "fdm", "타임스탬프": "2026-07-01T19

INFO Rest 클라이언트, 매핑 상태: 확인

INFO Rest 클라이언트, userBatch fdm에 대한 REST 게시 성공, 대기 시간 = 0, 현재 DC 시간 (UTC): 07/01/2026 19:47:34 USER logged at

INFO Rest 클라이언트, 에이전트 컨피그레이션 요청

FMC 로그

이 명령을 실행하여 에이전트에서 사용자-IP 매핑을 받았는지 확인합니다.

```
root@firepower123:/var/sf/user_enforcement# user_map_query.pl -u fdm

Current Time: 07/01/2026 11:36:03 UTC

Getting information on username(s)...


___
User #1: fdm
---

  ID:         10
  Last Seen:  Unknown
  for_policy: 1

==============================
|          Database          |
==============================

No IP Addresses


##) Group Name (ID)
 1) Domain Users (18)
 2) Users (48)
root@firepower123:/var/sf/user_enforcement#
```

fmc 출력

이전 명령에 매핑이 표시되지 않으면 이러한 로그를 수집하고 Cisco TAC에 문의하십시오.

FMC API에 대한 관련 로그 목록입니다. 돼지 꼬리 통나무는 그들 모두를 포함한다.

- /var/log/auth-daemon.log
- /var/log/messages
- /var/log/process_stdout.log
- /var/log/process_stderr.log

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.