

# 사용자 에이전트의 실시간 상태가 알 수 없음으로 표시됩니다

## 목차

[소개](#)

[증상](#)

[솔루션](#)

## 소개

Sourcefire User Agent를 구축한 후에는 모든 컨피그레이션 단계를 수행한 후에도 Real-Time Status(실시간 상태)를 알 수 없는 상태로 유지할 수 있습니다. 이 문서에서는 상태를 알 수 없음에서 사용 가능으로 변경하는 방법을 설명합니다.

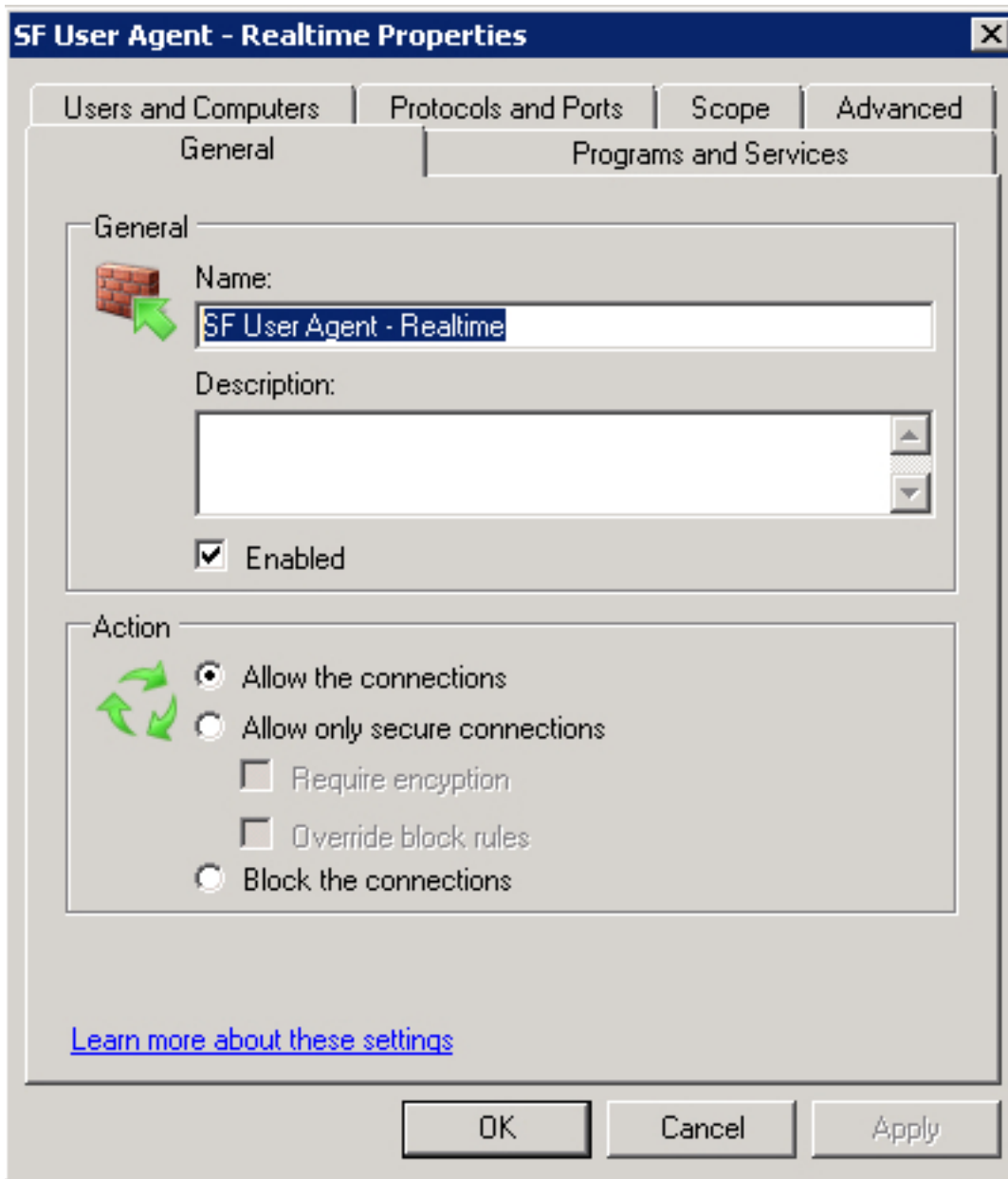
## 증상

도메인 컨트롤러의 방화벽 설정으로 인해 필요한 RPC 연결이 설정되지 않습니다. 사용자 에이전트는 RPC 동적 포트 연결을 사용하여 도메인 컨트롤러에 연결하고 실시간 모니터링을 설정합니다.

## 솔루션

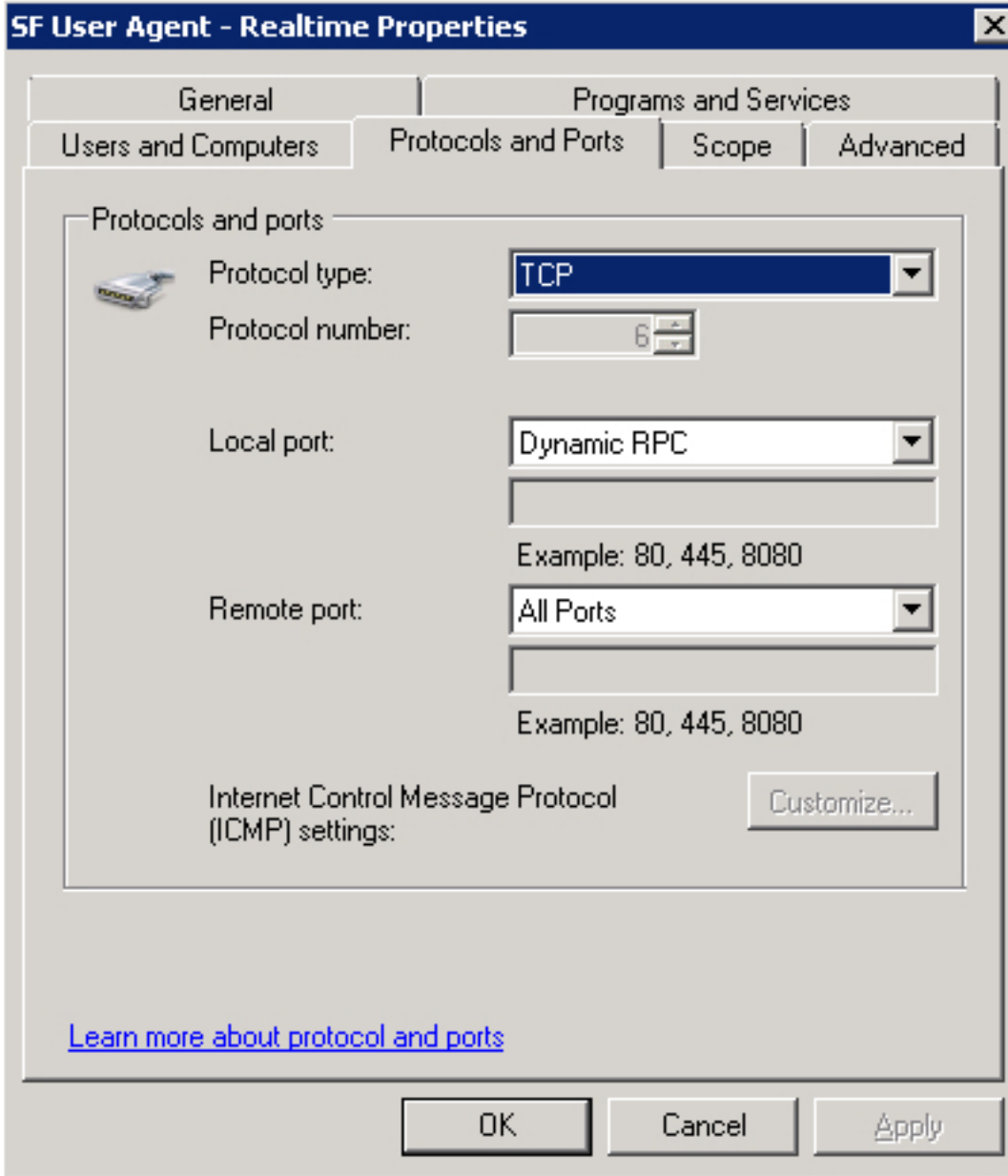
Windows 방화벽 및 고급 보안 콘솔을 사용하여 대상 도메인 컨트롤러에 인바운드 방화벽 규칙을 생성하여 사용자 에이전트에서 필요한 연결을 허용합니다. 다음은 설정 및 단계의 예입니다.

1. **General(일반)** 탭에서 규칙의 이름을 지정하고 Allow the Connections(연결 허용)를 선택합니다.

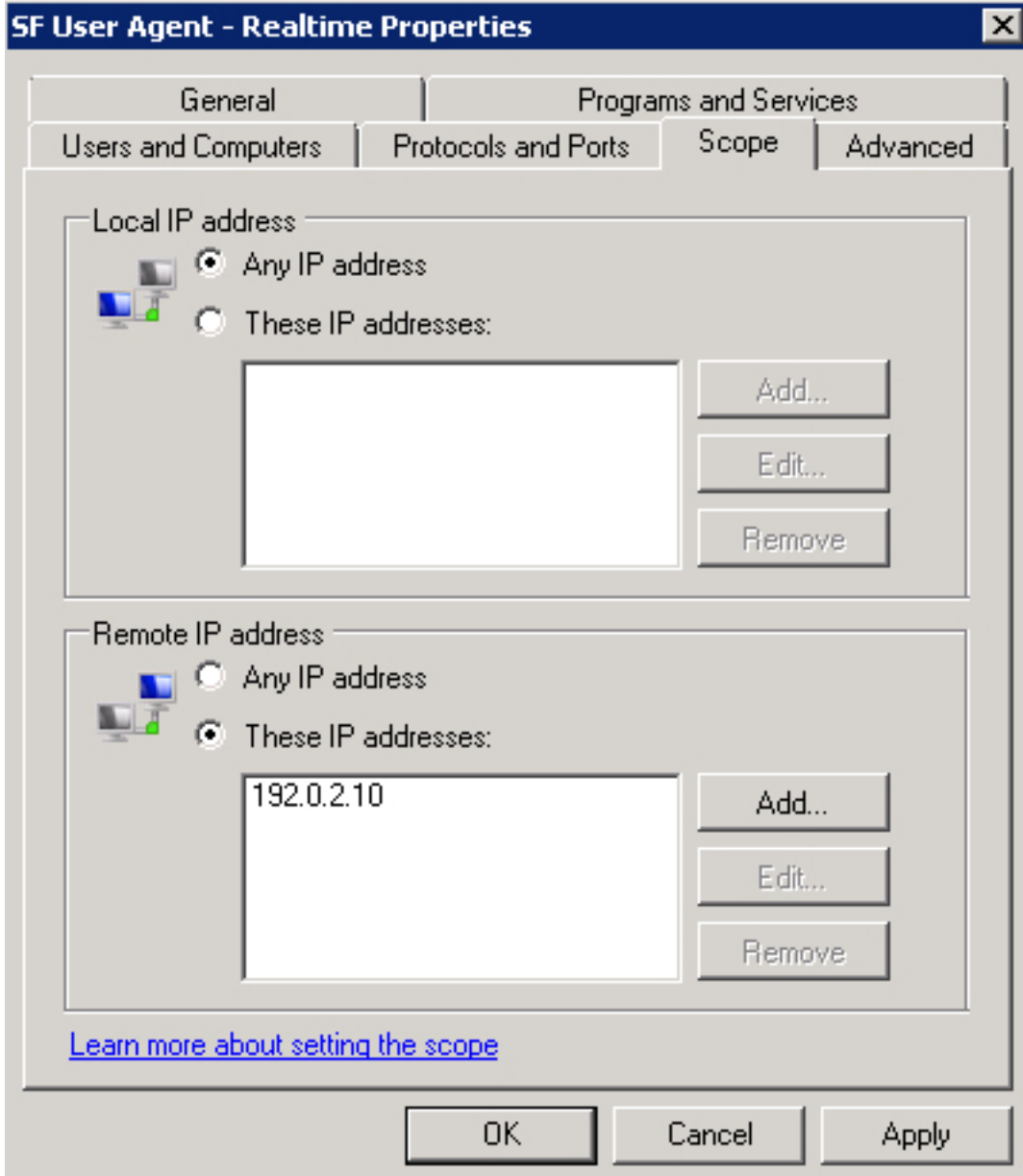


2. Protocols and Ports(프로토콜 및 포트) 탭에서 다음 항목을 선택합니다.

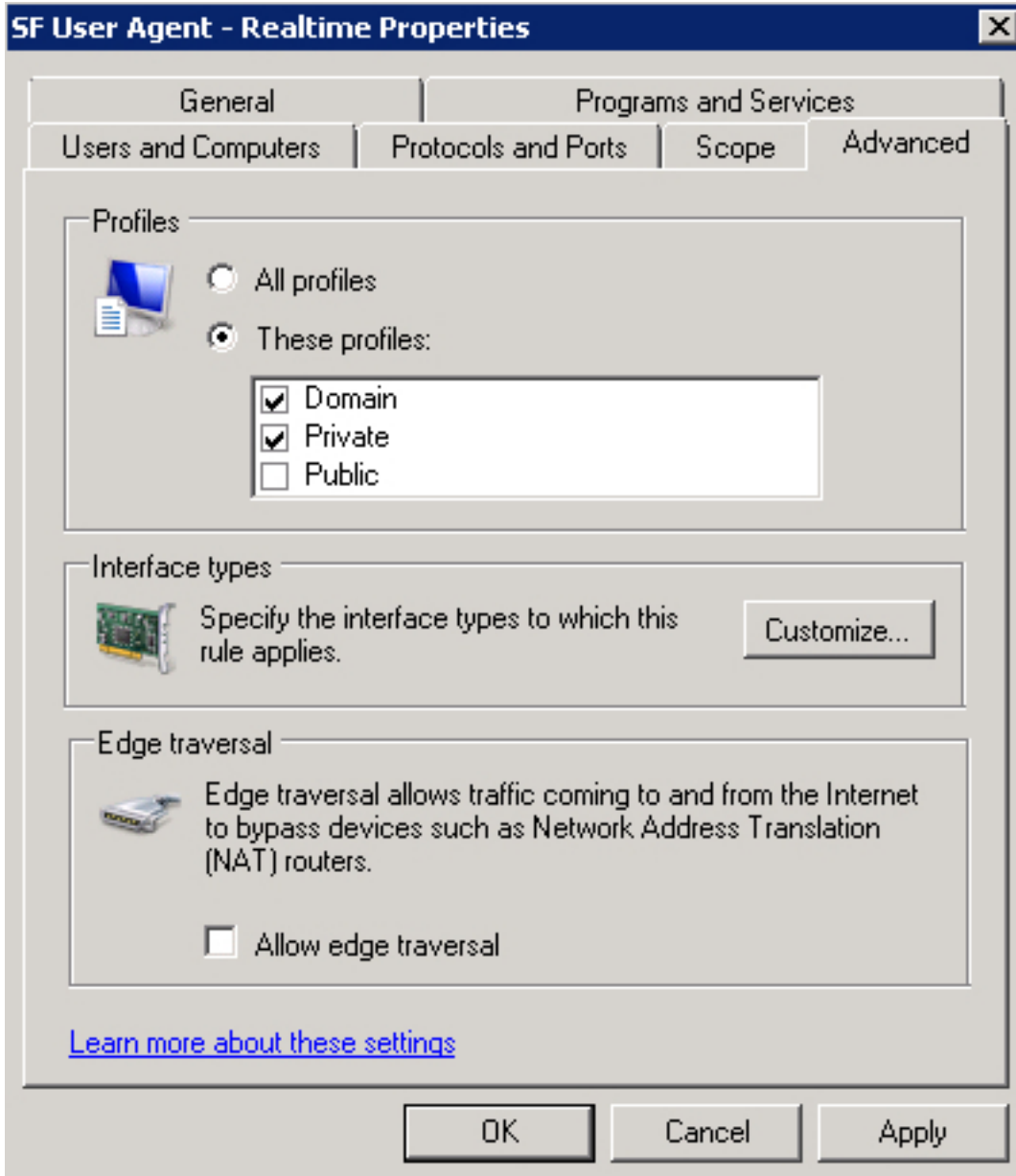
- 프로토콜 유형: TCP
- 로컬 포트: 동적 RPC
- 원격 포트: 모든 포트



3. **Scope(범위)** 탭에서 **Remote IP address(원격 IP 주소)**를 추가합니다. Add(추가)를 클릭하여 User Agent 호스트의 IP 주소를 입력합니다.



4. **Advanced(고급) 탭**에서 적절한 Profiles(프로파일)를 선택합니다.



방화벽 규칙을 저장하고 활성화한 다음 Sourcefire User Agent 서비스를 다시 시작합니다. 이제 실시간 연결 상태가 Unknown(알 수 없음)에서 **Available(사용 가능)**로 변경됩니다.