

ユーザ エージェントのリアルタイムのステータスが「Unknown」と表示される

目次

[概要](#)

[症状](#)

[解決策](#)

概要

Sourcefire User Agent の導入後にすべての設定手順を実行しても、リアルタイム ステータスは「Unknown」のままです。このドキュメントでは、ステータスを「Unknown」から「Available」に変更する手順について説明します。

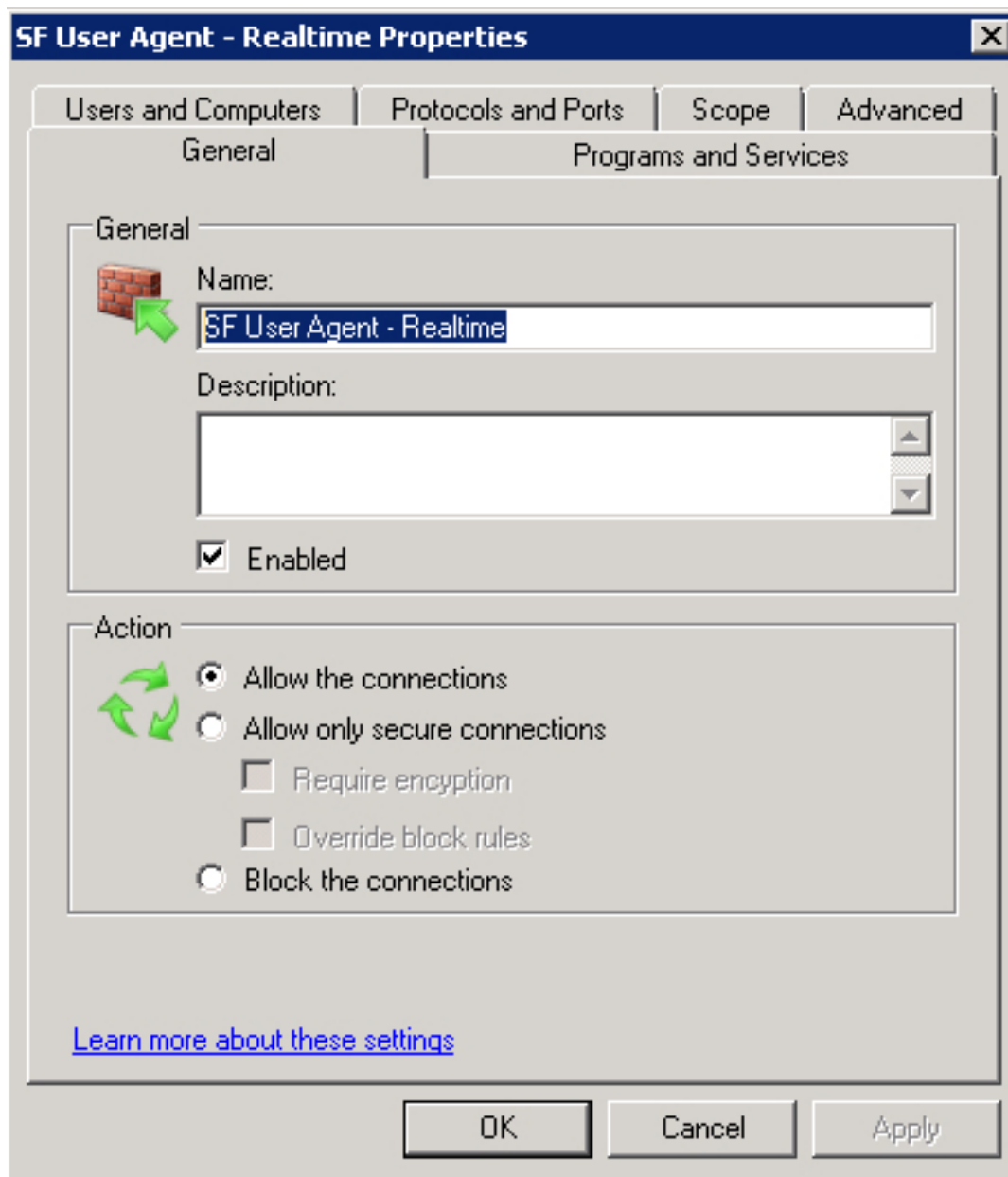
症状

ドメイン コントローラのファイアウォール設定によって、必要な RPC 接続の確立が妨げられています。User Agent は、RPC 動的ポート接続を使用してドメイン コントローラに接続し、リアルタイム モニタリングを確立します。

解決策

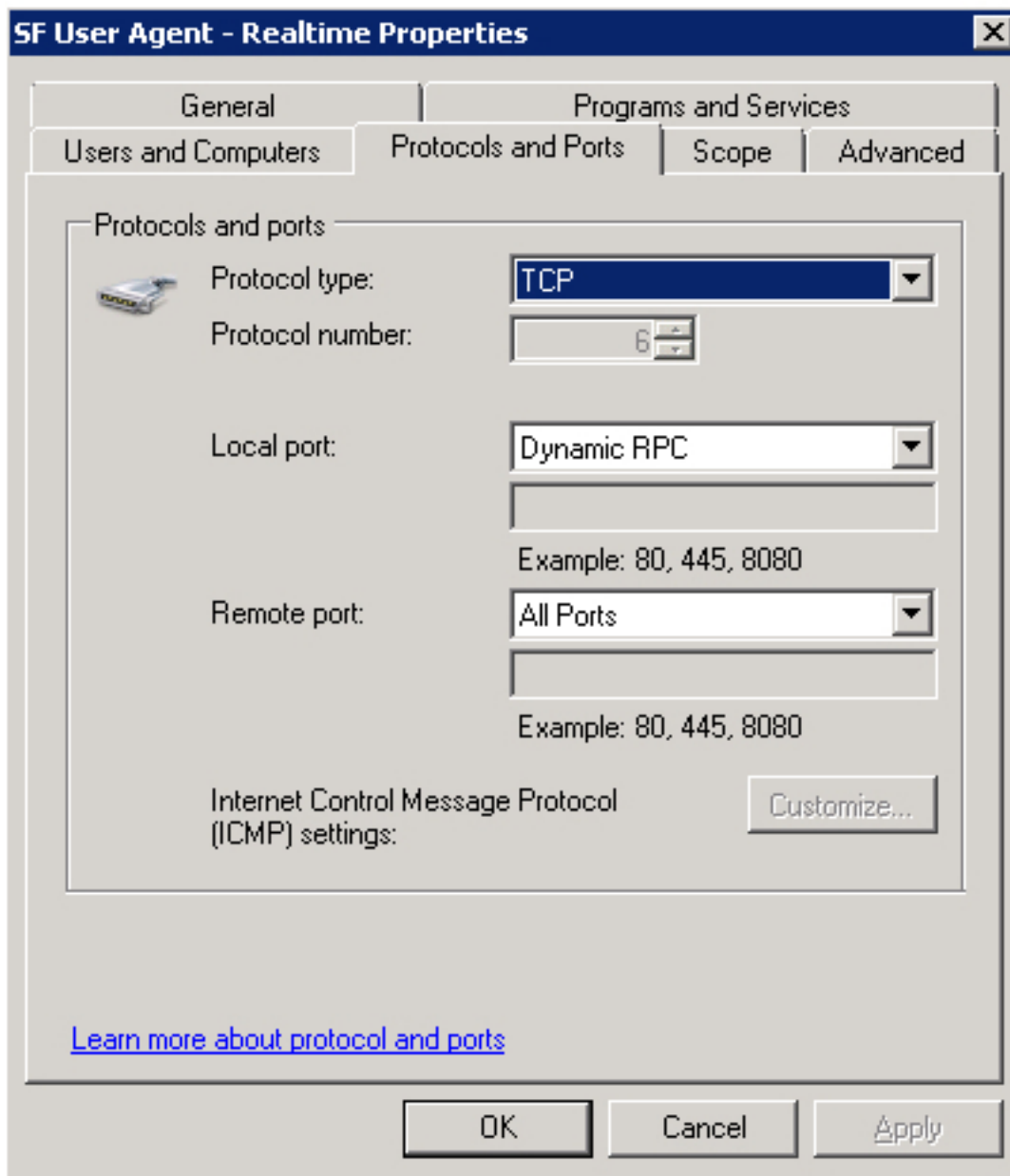
User Agent から必要な接続を確立できるように、目的のドメイン コントローラで [Windows Firewall with Advanced Security] コンソールを使用してインバウンド ファイアウォール ルールを作成します。設定例と手順を次に示します。

1. [General] タブで、ルールの名前を入力し、[Allow the Connections] を選択します。

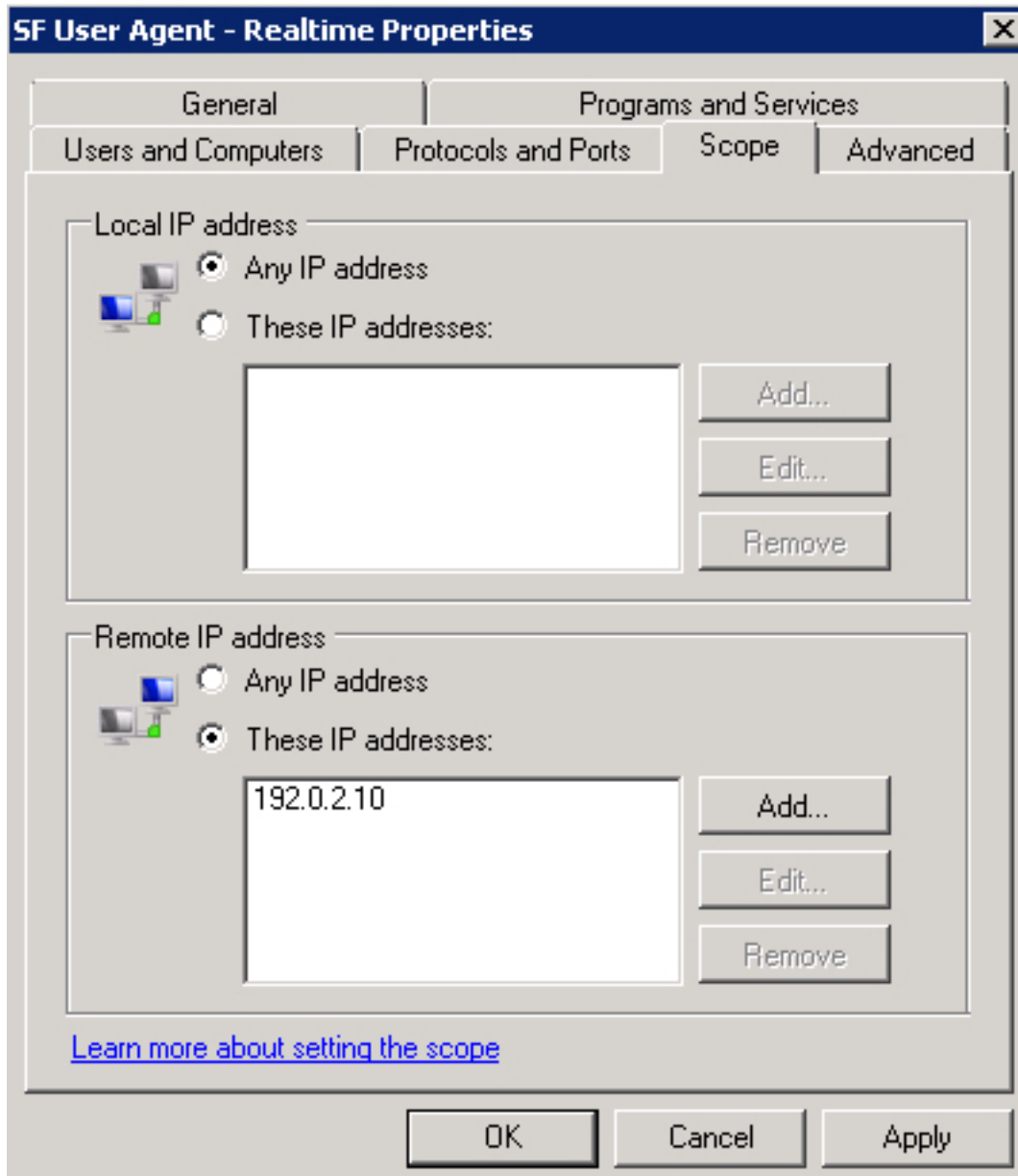


2. [Protocols and Ports] タブで以下の項目を選択します

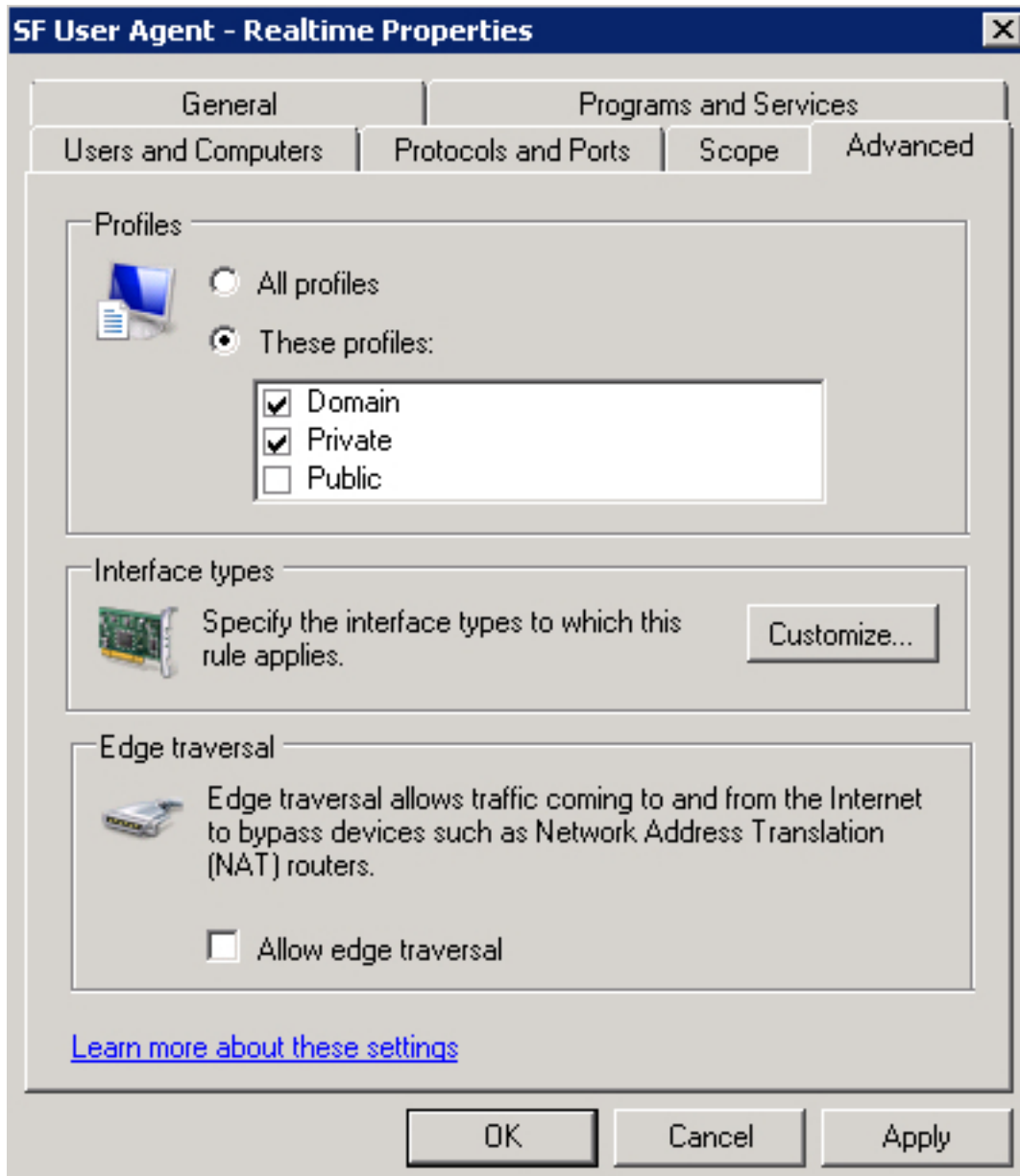
- Protocol type : TCP
- Local port : Dynamic RPC
- Remote port : All Ports



3. [Scope] タブでリモート IP アドレスを追加します。[Add] をクリックして、User Agent ホストの IP アドレスを入力します。



4. [Advanced] タブで適切なプロファイルを選択します。



ファイアウォールルールを保存して有効化し、Sourcefire User Agent サービスを再起動します。リアルタイム接続のステータスが [Unknown] から [Available] に代わっていることを確認してください。