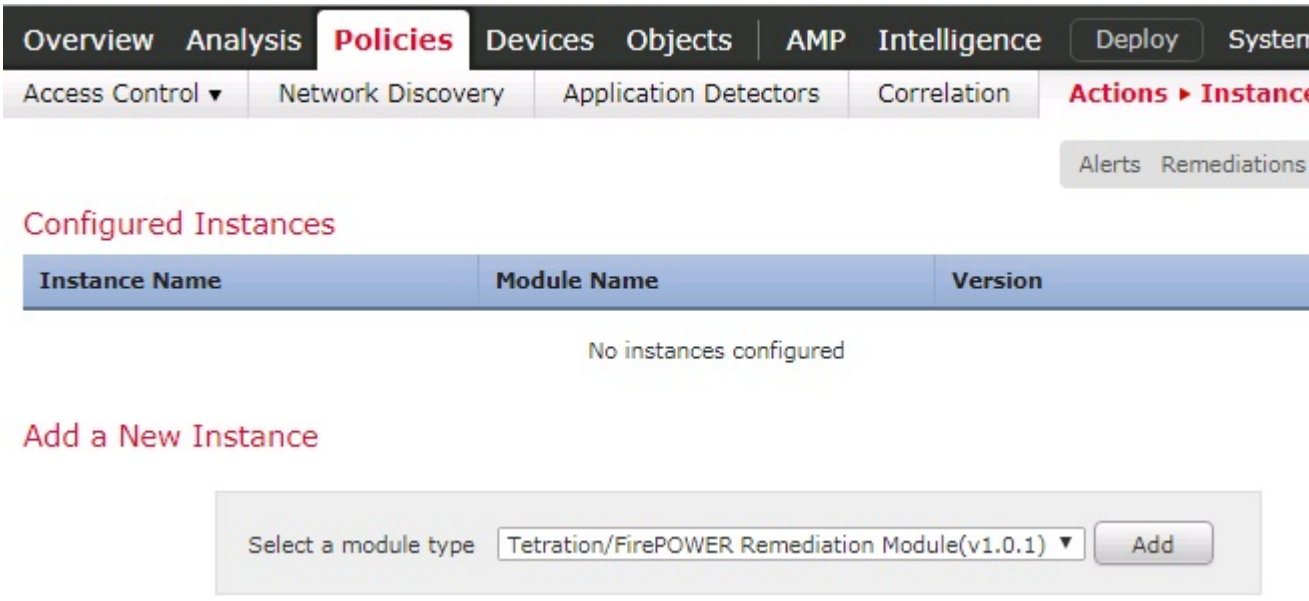
設定（Configure）

設定

FMC にインストールされた修復モジュールを設定するには、FMC GUI で次の手順を実行します。

ステップ 1 ネットワーク内の Tetration Analytics（TA）サーバごとに修復モジュールのインスタンスを作成します。

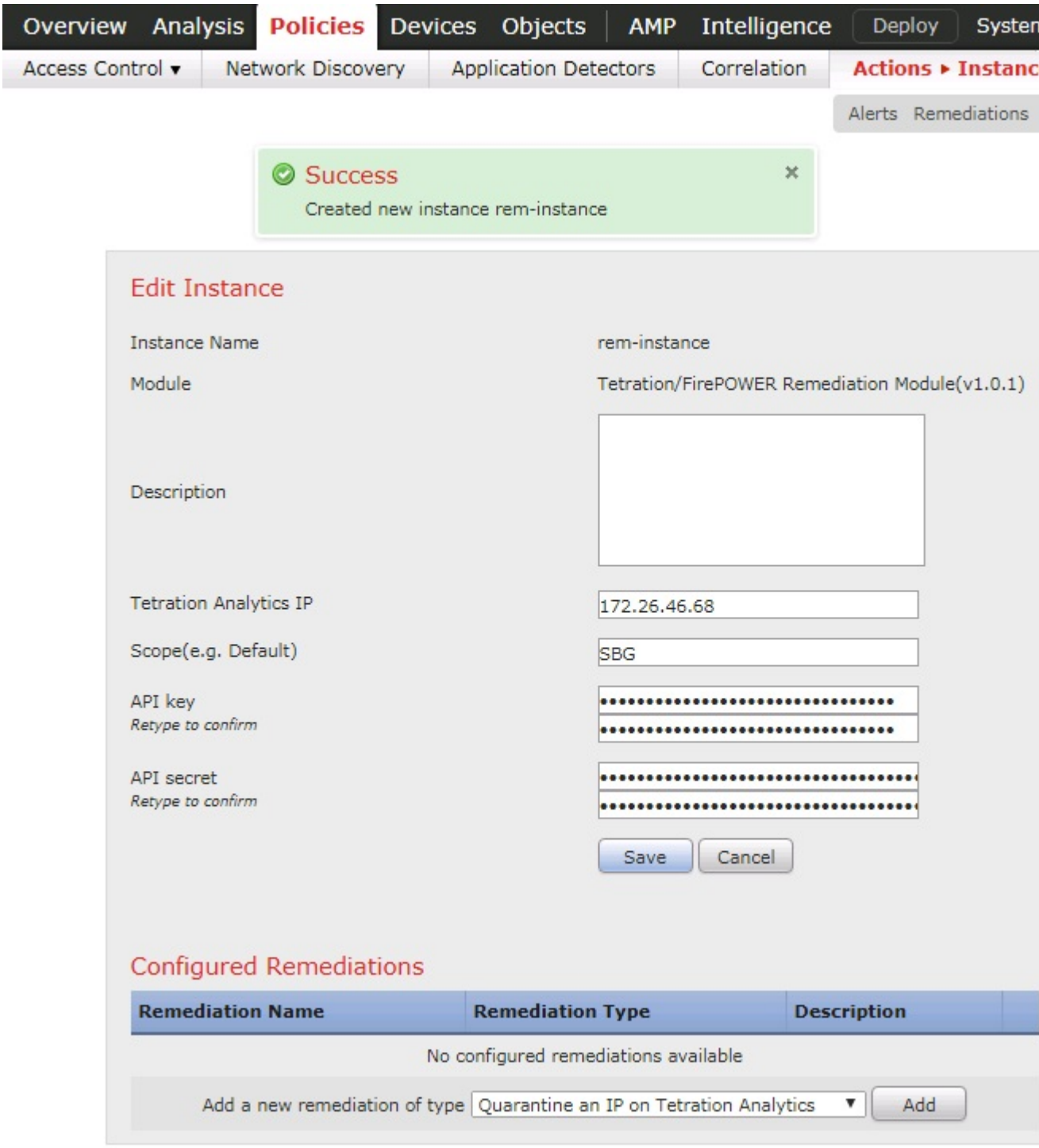
1. [ポリシー（Policies）] > [アクション（Actions）] > [インスタンス（Instances）] に移動します。
2. ドロップダウン リストから修復モジュールを選択し、[追加（Add）] をクリックします。



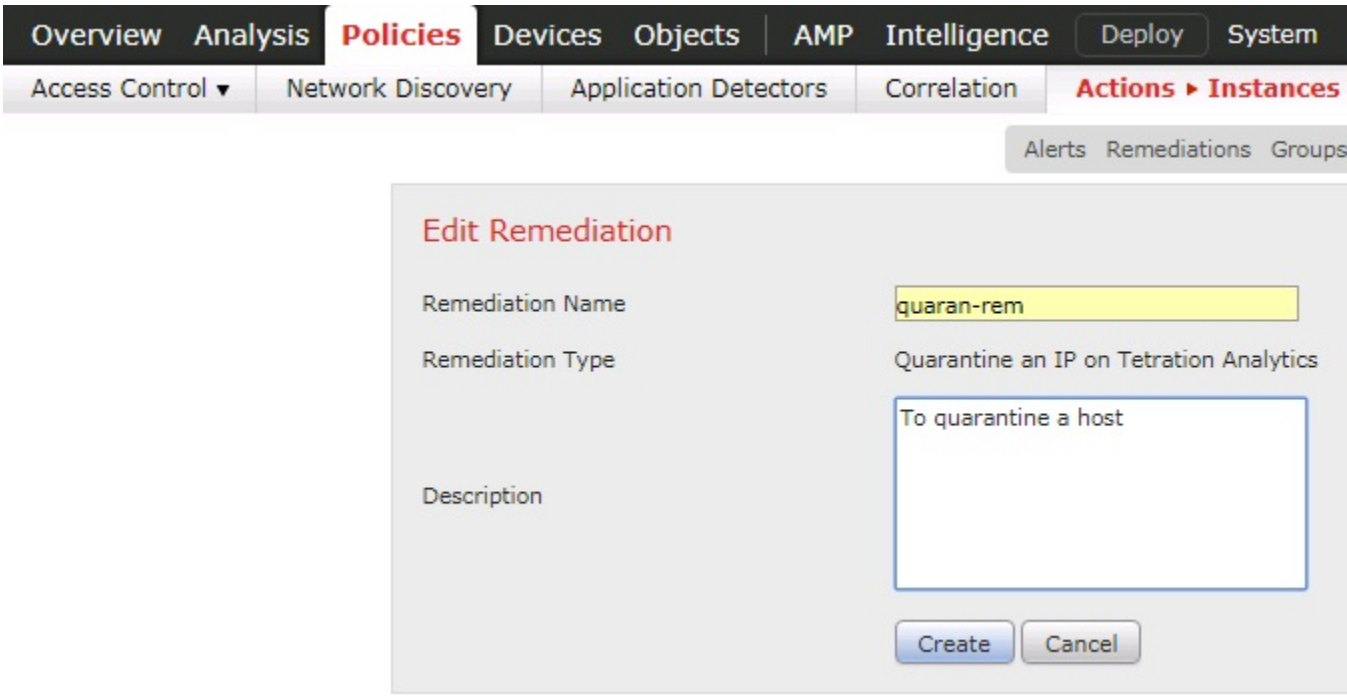
3. [インスタンス名（Instance Name）] を入力します（この例では、**rem-instance**）。

4. TA サーバの IP アドレス、API キー、API シークレット、および問題のある可能性のあるホストが含まれる範囲を入力します。[作成（Create）] をクリックします。

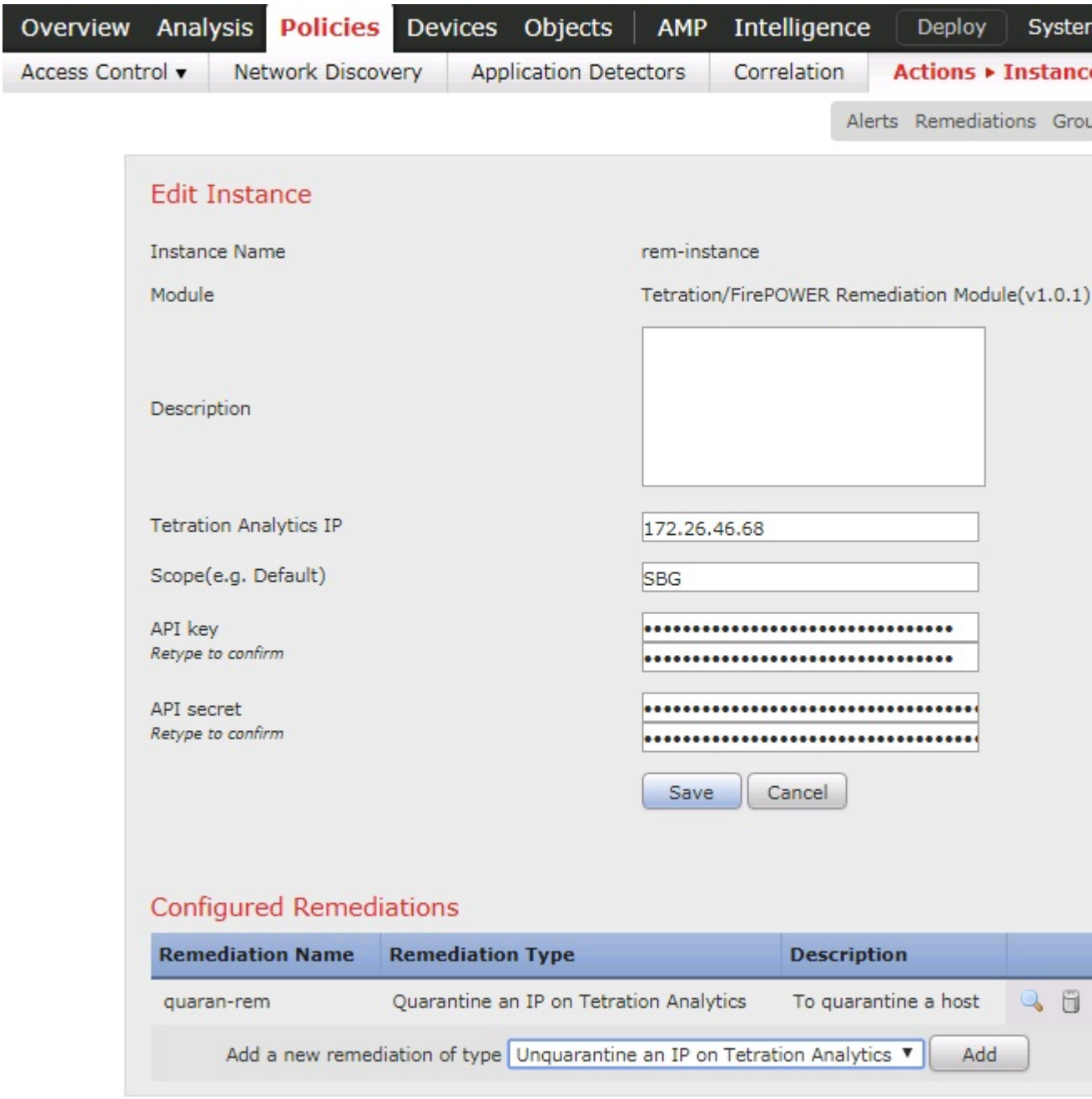
   （注） API キーとシークレットは、この時点では TA サーバに対して検証されません。サイト管理者、カスタマーサポート、またはルート スコープ オーナー ロールは、API キーとシークレットを TA で最初に作成しておく必要があります。ここで使用する情報をコピーします。詳細については、『 TA API Configuration Guide』を参照してください。



5. [設定されている修復（Configured Remediations）] で、修復のタイプを選択し（この例では、**Quarantine an IP on Tetration Analytics**）、[追加（Add）] をクリックして新しい修復を追加します。
6. [修復名（Remediation Name）] を入力し（この例では、**quaran-rem**）、[作成（Create）] をクリックします。



7. 設定した修復がテーブルに表示されます。[保存（Save）] をクリックします。



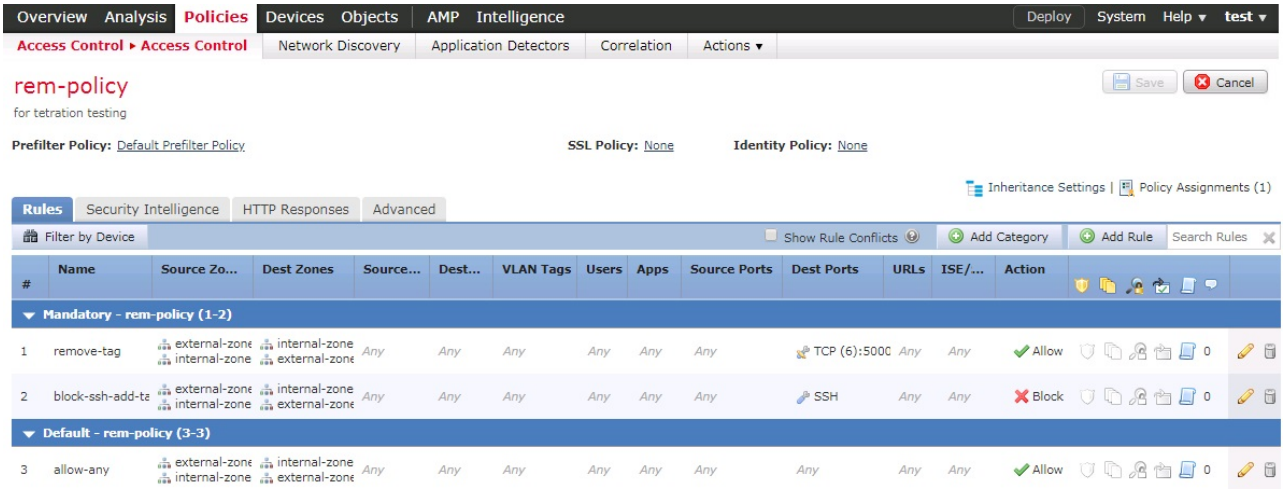
ステップ 2 アクセス制御ポリシーを設定します（この例では、**rem-policy**）。

1. [ポリシー（Policies）] > [アクセス制御（Access Control）] > [ルール（Rules）] に移動します。
2. [ルールの追加（Add Rule）] をクリックします（たとえば、**block-ssh-add-tag**）。
3. [アクション（Action）] で [ブロック（Block）] を選択します。

4. [ポート（Ports）] タブで、宛先ポートのプロトコルの一覧から [SSH] を選択し、[追加（Add）] をクリックします。
5. [保存（Save）] をクリックします。
6. [ロギング（Logging）] タブで、[接続開始時のログ（Log at Beginning of Connection）] を選択します。

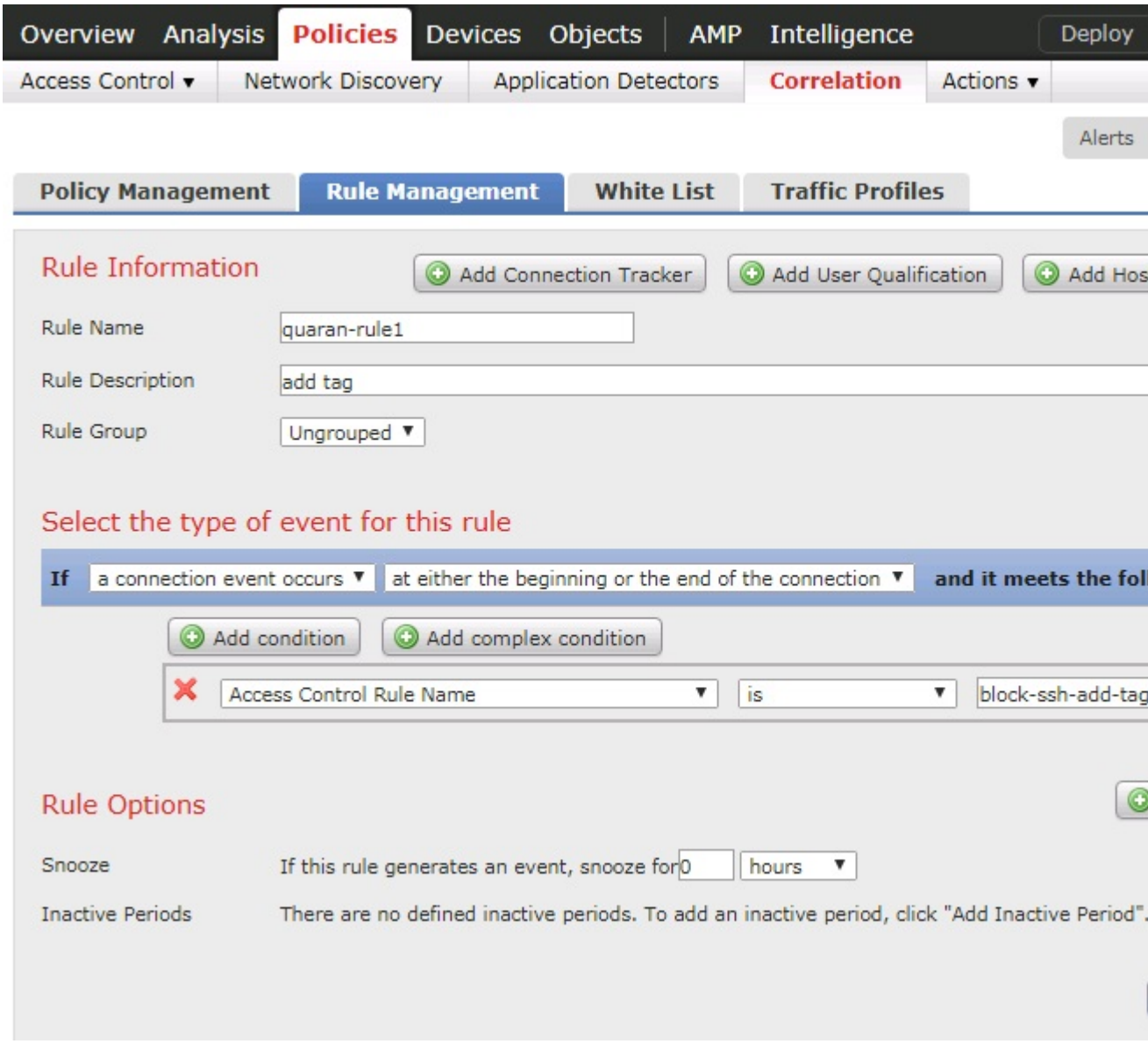
   重要　アクセスルールでロギングが有効になっていることを確認します。これにより、FMCはイベント通知を受信します。

7. [保存（Save）] をクリックします。



ステップ 3　相関ルールを設定します。

1. [ポリシー（Policies）] > [相関（Correlation）] > [ルールの管理（Rule Management）] に移動します。
2. [ルール名（Rule Name）] を入力し（この例では、**quaran-rule1**）、説明（オプション）を入力します。
3. [このルールのイベントタイプの選択（Select the type of event for this rule）] セクションで、[接続イベントの発生（a connection event occurs）] および [接続の開始時または終了時（at either the beginning or the end of the connection）] を選択します。
4. [条件を追加（Add condition）] をクリックし、演算子を **OR** から **AND** に変更します。
5. ドロップダウンリストで、[アクセスコントロールルール名（Access Control Rule Name）]、[は（is）] を選択し、ステップ 2 で設定したアクセス コントロール ルールの名前を入力します（この例では、**block-ssh-add-tag**）。

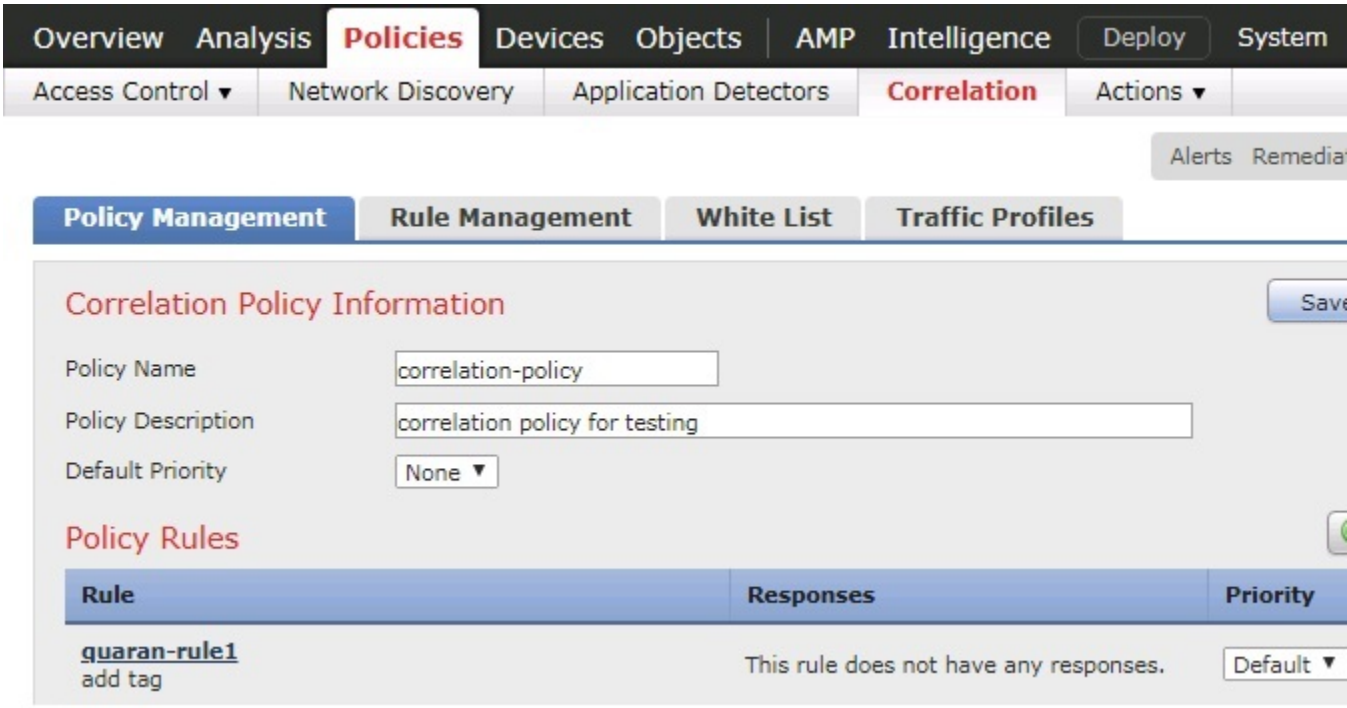


6. [保存（Save）] をクリックします。

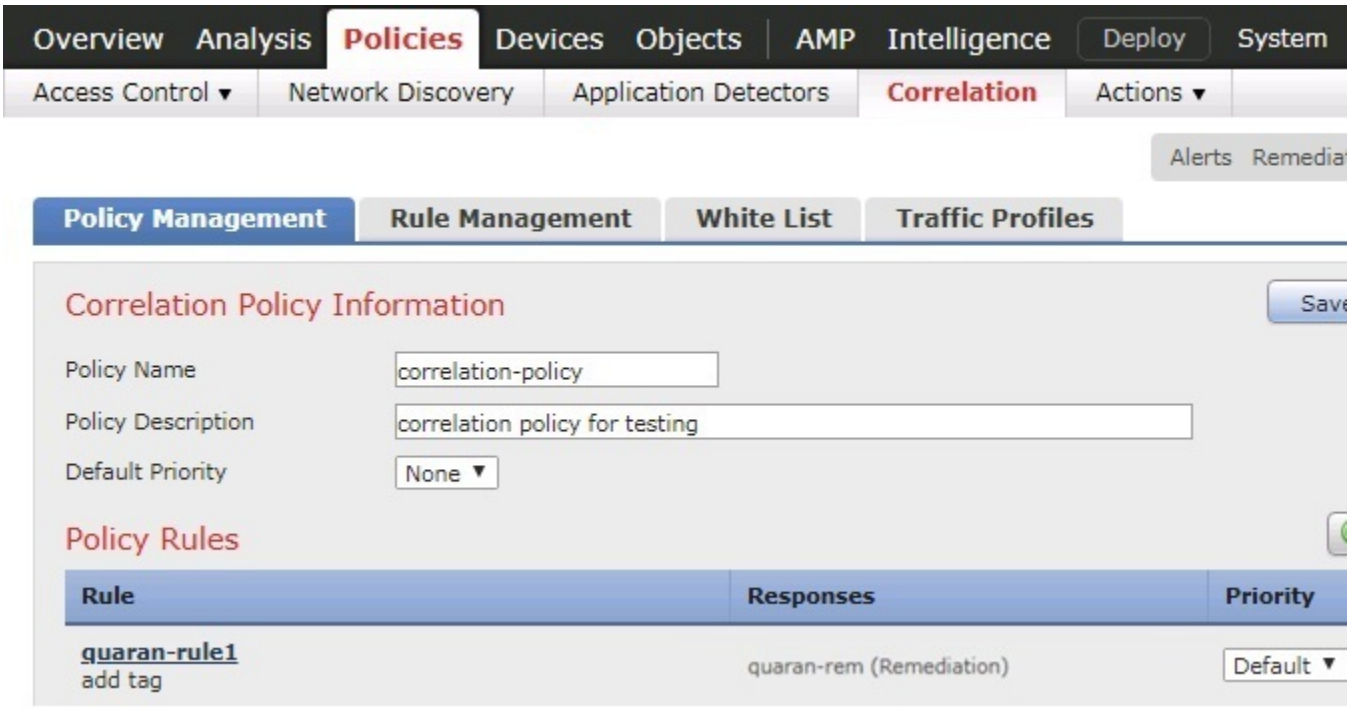
ステップ 4 相関ルールに、修復モジュールのインスタンスを応答としてアソシエートします。

1. [ポリシー（Policies）]>[相関（Correlation）]>[ポリシーの管理（Policy Management）] に移動します。
2. [ポリシーの作成（Create Policy）] をクリックします。
3. [ポリシー名（Policy Name）] を入力し（この例では、**`correlation-policy`**）、説明（オプション）を入力します。
4. [Default Priority] ドロップダウンリストから、ポリシーのプライオリティを選択します。[なし（None）] を選択して、ルールのプライオリティのみ使用します。

5. [ルールの追加（Add Rules）] をクリックし、ステップ 3 で設定した相関ルールを選択し（この例では、**quaran-rule1**）、[追加（Add）] をクリックします。



6. ルールの横にある [応答（Responses）] アイコンをクリックし、ルールに応答を割り当てます（この例では、**quaran-rem**）。[更新（Update）] をクリックします。



7. [保存（Save）] をクリックします。