ISE を使用した FirePOWER 6.1 pxGrid 修復の設定

目次

[はじめに](#)
[前提条件](#)
[要件](#)
[使用するコンポーネント](#)
[設定](#)
[ネットワーク図](#)
[Firepower を設定して下さい](#)
[ISE の設定](#)
[確認](#)
[トラブルシューティング](#)
[関連情報](#)

概要

この資料に Identity Services Engine （ ISE ）で Firepower 6.1 pxGrid 治療を設定する方法を記述されています。 ISE エンド ポイント保護 サービス (EPS) と Firepower 6.1+ ISE 治療モジュールがネットワーク アクセス レイヤの攻撃者の qurantine/ブラックリストに載せることを自動化するのに使用することができます。

前提条件

要件

Cisco では、次の項目について基本的な知識があることを推奨しています。

- Cisco ISE
- Cisco Firepower

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Cisco ISE バージョン 2.0 パッチ 4
- Cisco Firepower 6.1.0
- バーチャル ワイヤレス LAN コントローラ (vWLC) 8.3.102.0

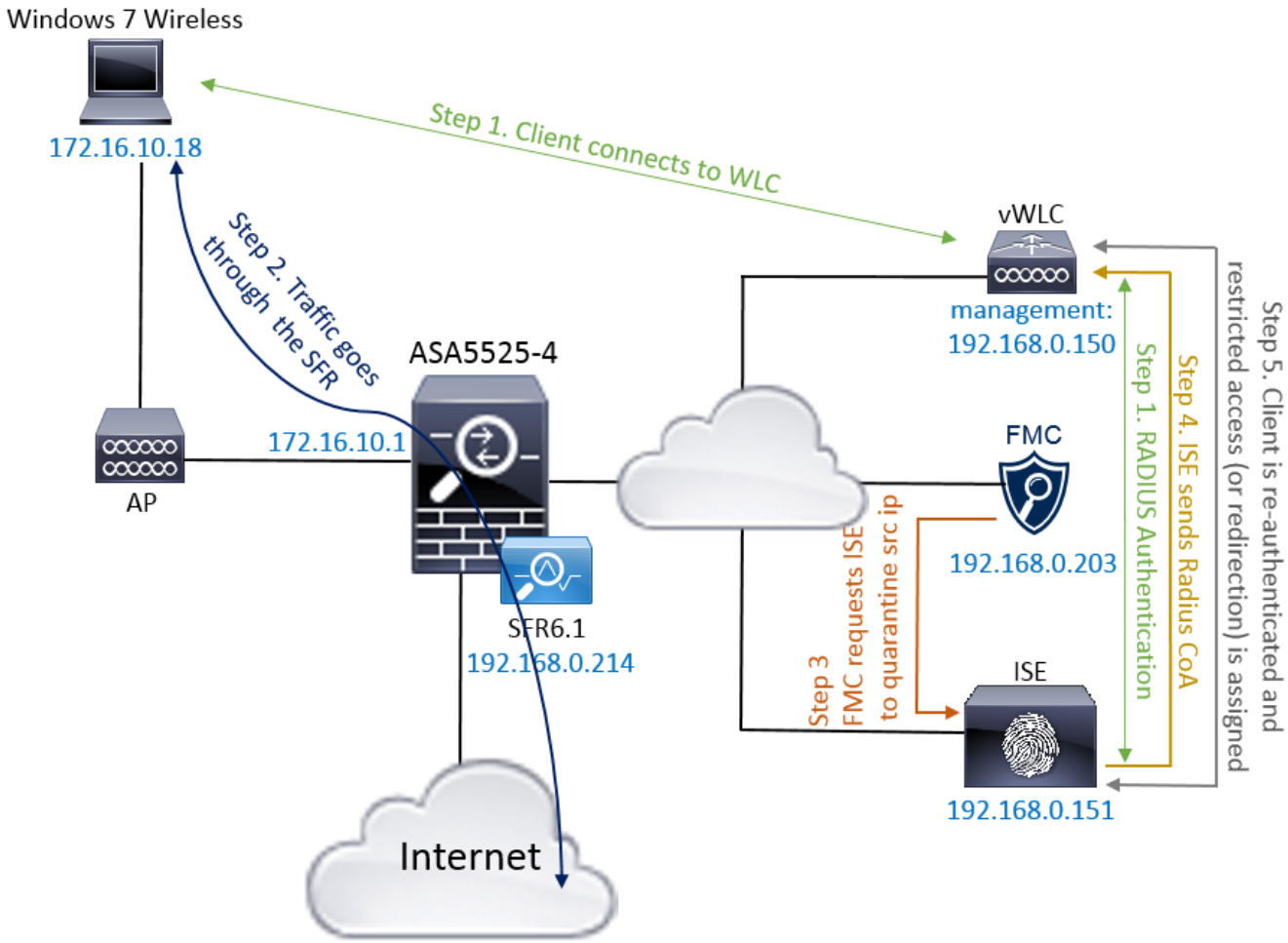
本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、初期 (デフォルト) 設定の状態から起動しています。 稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

設定

この技術情報は Firepower で ISE 統合の初期設定を、Active Directory （ AD ）の ISE 統合、AD の Firepower 統合カバーしません。 References セクションへのこの情報ナビゲートに関しては。 相関 ルールが一致する場合の治療として ISE EPS 機能（検疫、unquarantine、ポート シャットダウン）を使用する Firepower 6.1 治療モジュール割り当て Firepower システム。

注: ポート シャットダウンはワイヤレス配備に利用できません。

ネットワーク図



フロー説明:

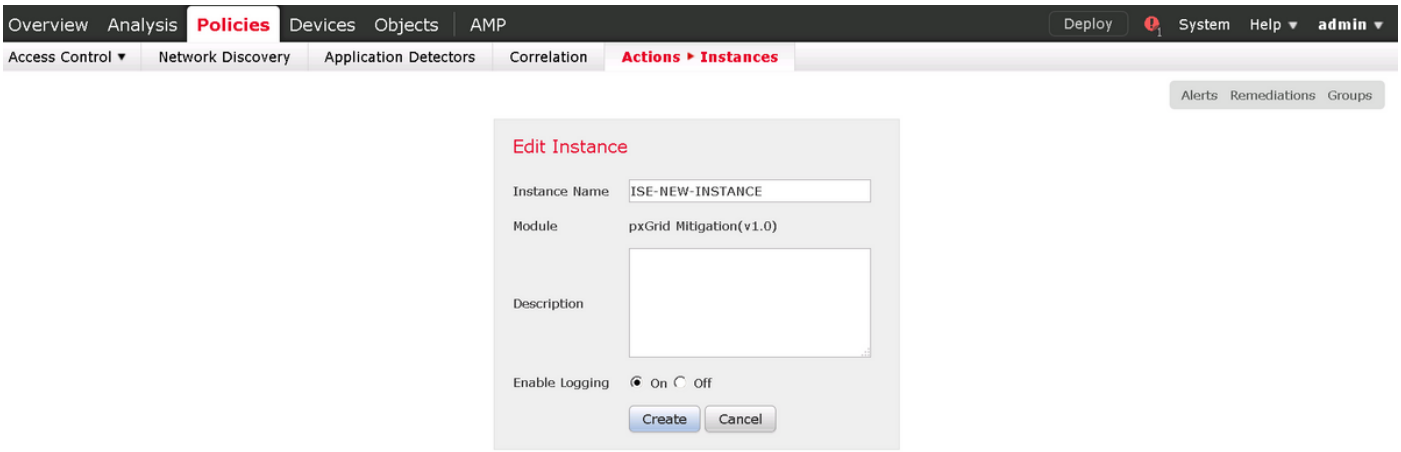
1. クライアントはネットワークに接続し、ISE と認証を受け、ネットワークに無制限のアクセスを認める許可プロファイルの承認規則を見つけます。
2. クライアントからのトラフィックは Firepower デバイスをそれからフローします。
3. ユーザは悪意のあるアクティビティを行い始め、pxGrid によって ISE 治療をするためにそれから Firepower Management Center （ FMC ）を誘発する相関 ルールを見つけます。
4. ISE はエンド ポイントに EPSStatus 検疫を割り当て、ネットワーク アクセス デバイスへの許可の半径変更を誘発します（ WLC かスイッチ）。
5. クライアントは制限された アクセス（変更 SGT かポータルまたは拒否アクセスへのリダイレクト）を割り当てる別の承認ポリシーを見つけます。

注: ネットワーク アクセス デバイス (NAD) はエンド ポイントに IP アドレスをマップするのに使用されている IP アドレス情報をそれに与えるために説明する ISE に RADIUS を送信するために設定する必要があります。

Firepower を設定して下さい

ステップ 1. pxGrid 軽減例を設定して下さい。

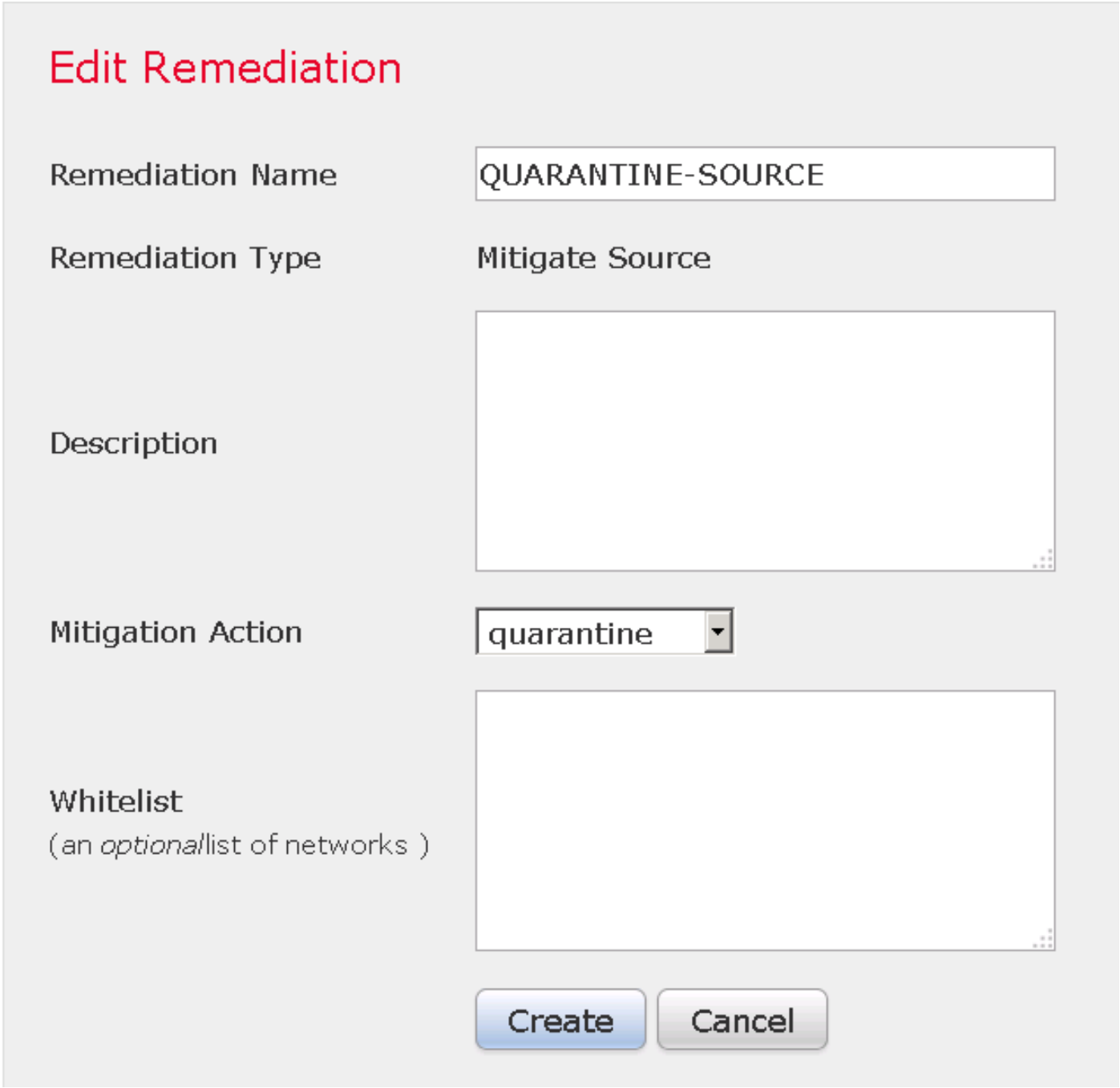
ポリシー > 操作 > 例にナビゲート し、イメージに示すように pxGrid 軽減例を追加して下さい。



ステップ 2.治療を設定して下さい。

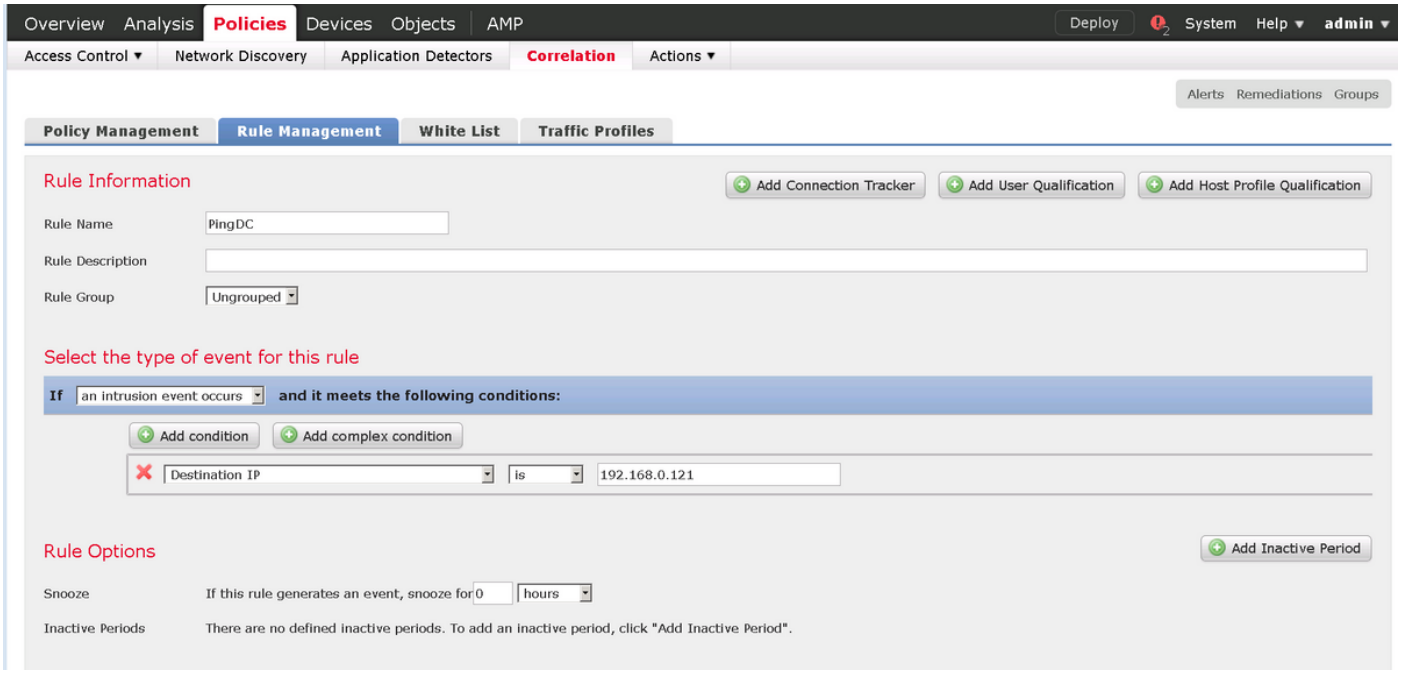
利用可能な 2 つの型があります: 宛先を軽減し、ソースを軽減して下さい。 このソース例で軽減は使用されます。 治療型を選択し、**イメージに示すように『Add』 をクリック して下さい:**

イメージに示すように治療に軽減操作を割り当てて下さい:



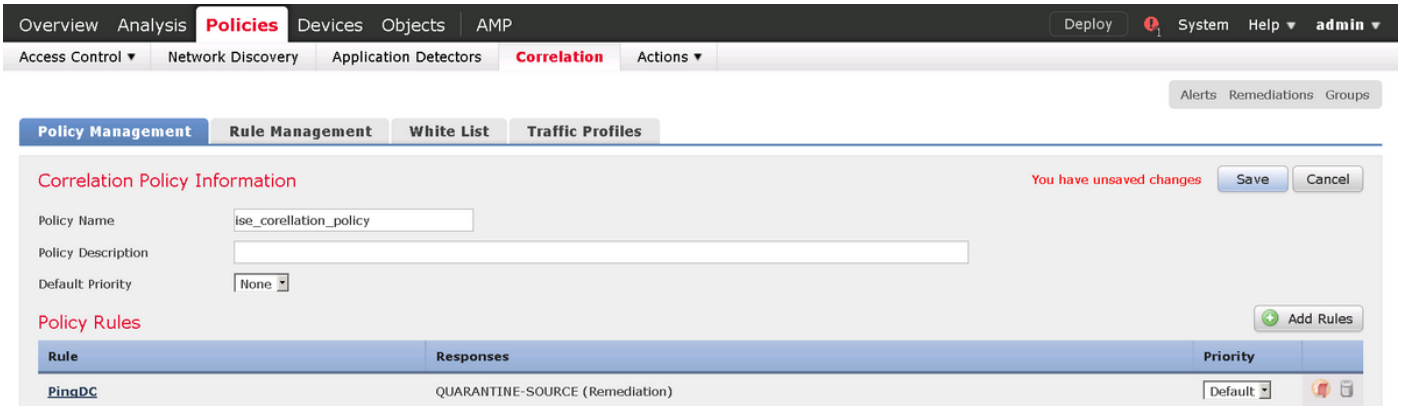
ステップ 3.相関 ルールを設定して下さい。

ナビゲート し、**ルール**相関 ルールをあります起こる治療のためのトリガーは**ポリシー > 相関 > ルール管理**に『Create』 をクリック します。 相関 ルールは複数の状態が含まれている場合があります。 この相関 ルール例で **PingDC は**不正侵入イベントが発生し、宛先 IP アドレスが 192.168.0.121 なら場合見つかります。 カスタム不正侵入ルール一致する ICMP工コー応答はイメージに示すようにテストの為に設定されます:

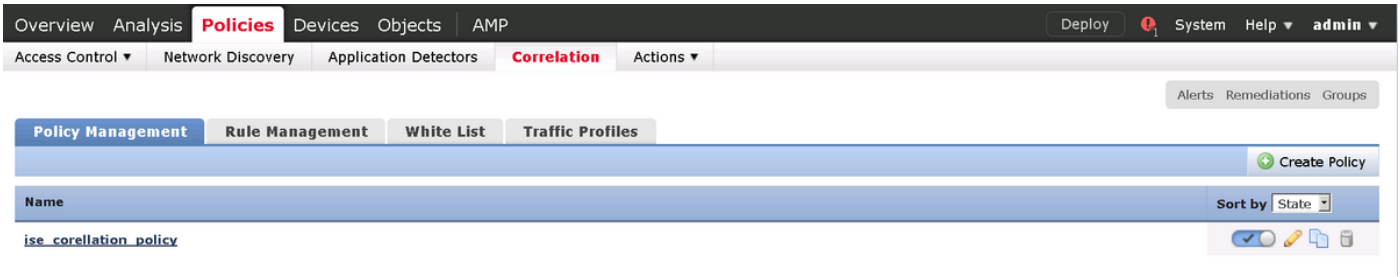


ステップ 4.相関ポリシーを設定して下さい。

ポリシー > 相関 > ポリシー管理へのナビゲートはおよび**ポリシーを**『Create』 をクリック し、ポリシーにルールを追加し、イメージに示すようにそれへの応答を割り当てます:



イメージに示すように相関ポリシーを有効に して下さい:

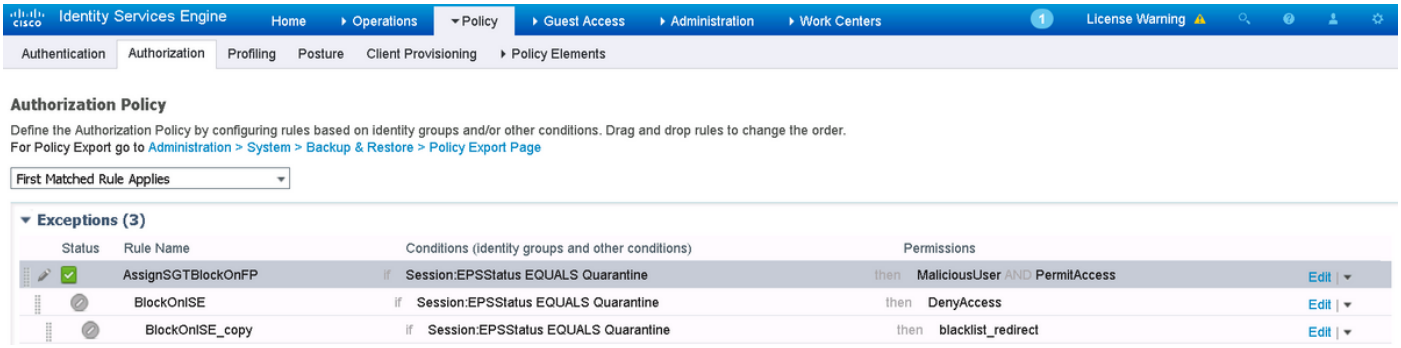


ISE の設定

ステップ 1.承認ポリシーを設定して下さい。

ポリシー > 許可にナビゲート し、治療が起こった後見つかる新しい承認ポリシーを追加して下さい。 使用**セッション: EPSStatus は**状態として**検疫に匹敵します。** その結果使用することができる複数のオプションがあります:

- 割り当てアクセスは異なる SGT を割り当て、（ネットワークデバイスのアクセス制御制限を適用して下さい）
- アクセスを拒否して下さい（ユーザはネットワークから蹴り、再度接続できないはずです）
- **ブラックリスト** ポータルへのリダイレクト（このシナリオ カスタム ホットスポット ポータルでこのために設定されます

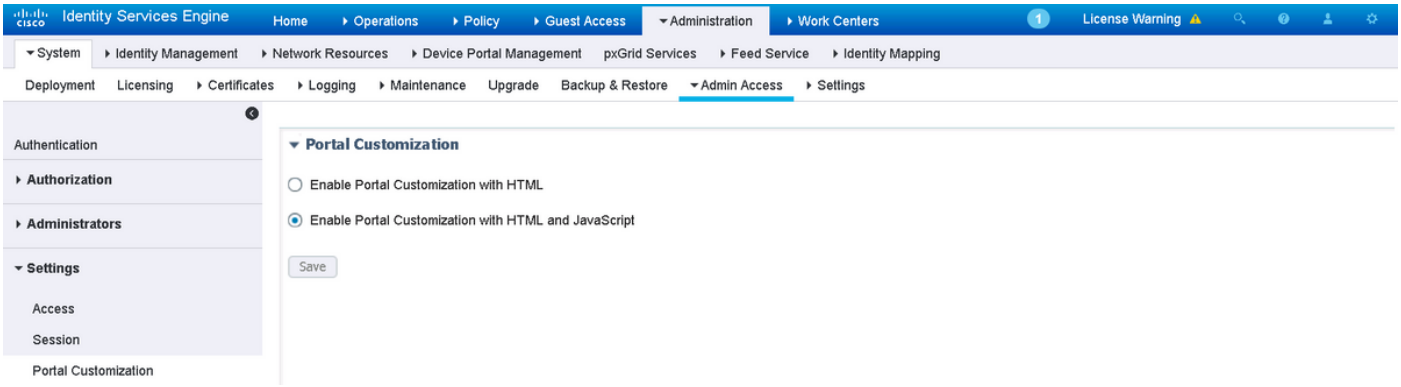


カスタム門脈設定

この例では、ホットスポット ポータルは**ブラックリスト**で設定されます。 カスタム テキストが付いている Acceptable Use Policy （AUP）ページだけあり、AUP を受け入れる可能性がありません（これはジヤバスクリプトとされます）。 これを実現させるために、最初にジヤバスクリプトを使用可能にし、次に門脈カスタマイゼーション設定に AUP ボタンおよび制御を隠すコードを貼り付ける必要があります。

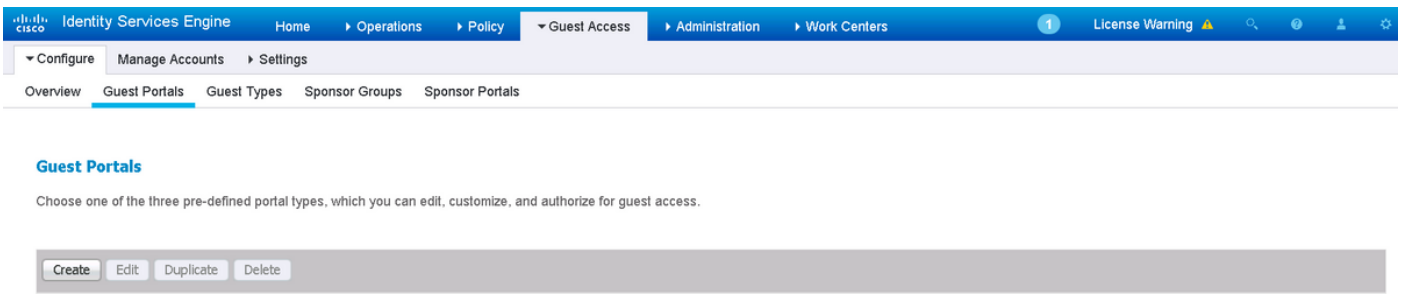
ステップ 1.イネーブル ジヤバスクリプト。

Administration > システム > Admin Access> 設定へのナビゲート **> 門脈カスタマイゼーション。HTML およびジヤバスクリプトの門脈カスタマイゼーションを**『Enable』 を選択 し、『SAVE』 をクリック して下さい。



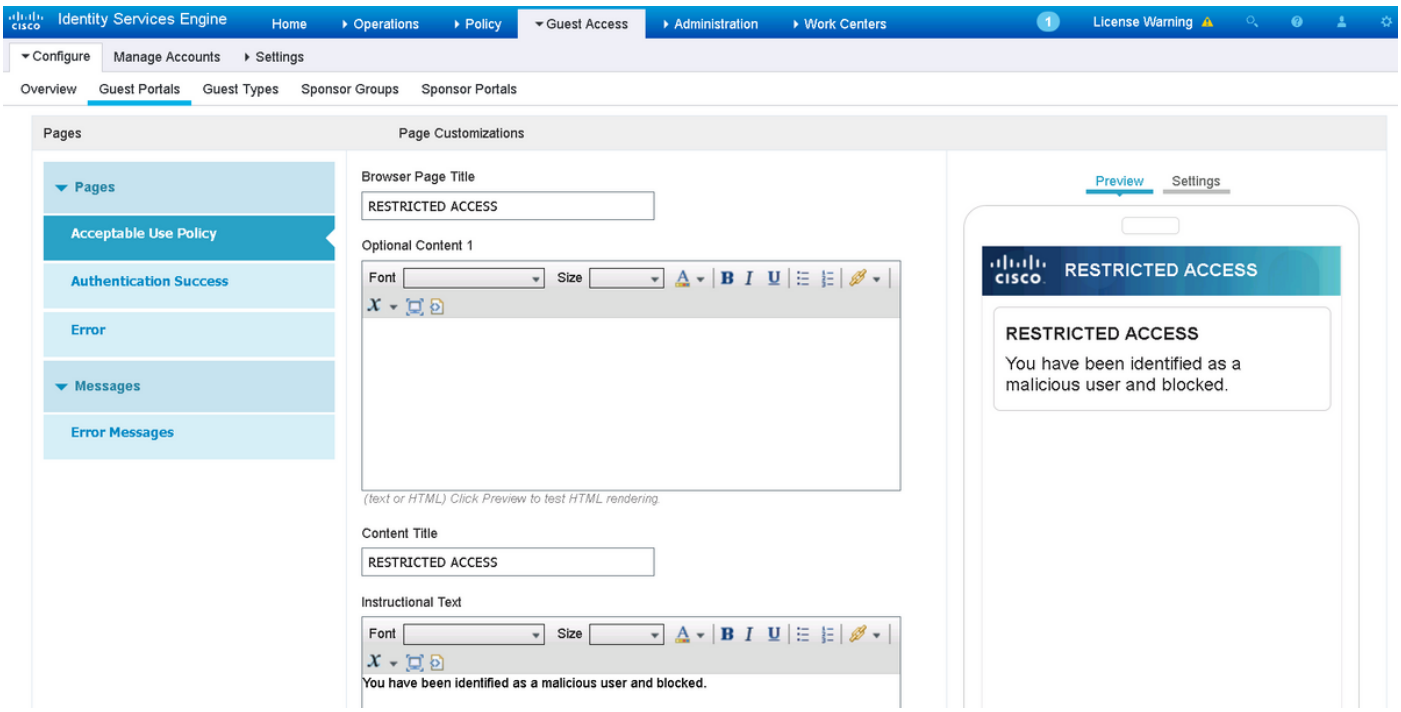
ステップ 2.ホットスポット ポータルを作成して下さい。

ゲスト アクセスへのナビゲートは **> > ゲスト ポータル設定し、**『Create』 をクリック しましたり、そしてホットスポット型を選択します。



ステップ 3.門脈カスタマイゼーションを設定して下さい。

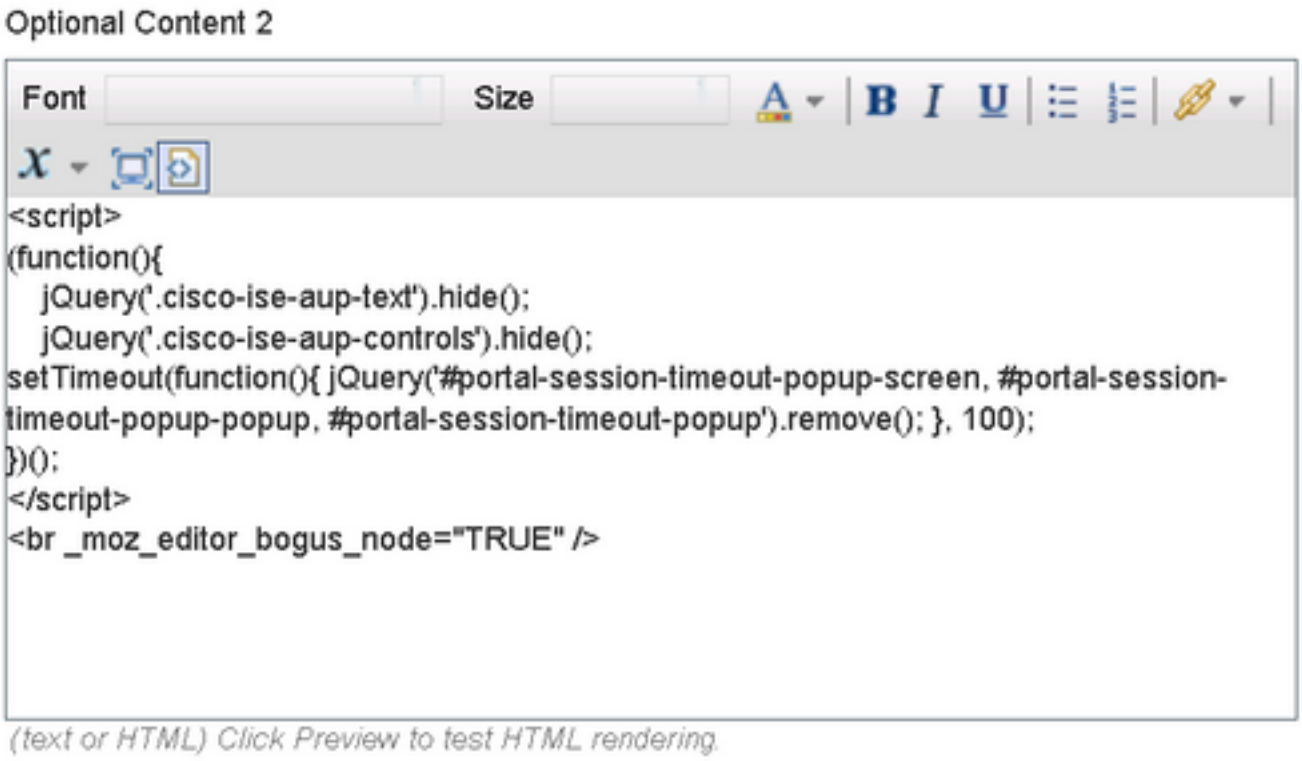
門脈ページ カスタマイゼーションにナビゲート し、ユーザに適切な警告を提供するためにタイトルおよび内容を変更して下さい。



オプション内容 2 にスクロールし、**HTML ソースを**『toggle』 をクリック し、スクリプト内部を貼り付けて下さい:

```
<script> (function(){ jQuery('.cisco-ise-aup-text').hide(); jQuery('.cisco-ise-aup-controls').hide(); setTimeout(function(){ jQuery('#portal-session-timeout-popup-screen, #portal-session-timeout-popup-popup, #portal-session-timeout-popup').remove(); }, 100); })(); </script>
```

Untoggle HTML ソースをクリックして下さい。



確認

設定が適切に機能することを確認するために、この項に記載する情報を活用してください。

Firepower

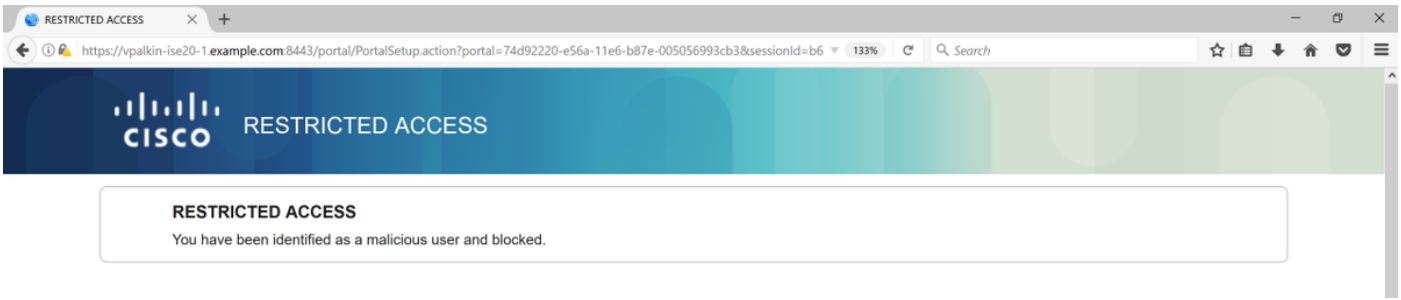
起こる治療のためのトリガーは相関ポリシー/ルールのヒットです。 **分析 > 相関 > 相関イベント**にナビゲート し、相関イベントが起こったことを確認して下さい。

ISE

ISE はそれから Radius を誘発する必要があります: CoA はユーザを、これらのイベント確認された作動中である場合もあります **> RADIUS Livelog** 再認証し。

この例では、ISE はエンド ポイントに異なる SGT **MaliciousUser を**割り当てました。 **拒否アクセス**許可プロファイルの場合にはユーザは無線接続を失い、再度接続できません。

ブラックリスト ポータルとの治療。 治療承認規則がポータルにリダイレクトするために設定される場合攻撃者観点からこのようになる必要があります:



トラブルシューティング

このセクションでは、設定のトラブルシューティングに役立つ情報を提供します。

このイメージに示すように**分析 > 相関 > ステータス**にナビゲート して下さい。

結果メッセージは**治療の正常な完了**か特定のエラーメッセージを返す必要があります。 syslog を確認して下さい: **システム > モニタリング > Syslog** およびフィルタは **pxgrid** と出力しました。同じログは **/var/log/messages** で確認することができます。

関連情報

- https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/200319-Troubleshoot-ISE-and-FirePOWER-Integrati.html
- https://communities.cisco.com/docs/DOC-68284
- https://communities.cisco.com/docs/DOC-68285
- https://communities.cisco.com/thread/64870?start=0&tstart=0
- http://www.cisco.com/c/en/us/td/docs/security/ise/2-0/admin_guide/b_ise_admin_guide_20.html
- http://www.cisco.com/c/en/us/td/docs/security/firepower/610/configuration/guide/fpmc-config-guide-v61.html