Konfigurieren der Firepower 6.1 pxGrid-Problembehebung mit der ISE

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie die Firepower 6.1 pxGrid-Problembehebung mit der Identity Services Engine (ISE) konfiguriert wird. Das FirePOWER 6.1+ ISE-Sanierungsmodul kann zusammen mit dem ISE Endpoint Protection Service (EPS) verwendet werden, um Quarantäne-/Blacklisting von Angreifern auf dem Netzwerkzugriffs-Layer zu automatisieren.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über grundlegende Kenntnisse in folgenden Bereichen zu verfügen:

- Cisco ISE
- Cisco FirePOWER

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco ISE Version 2.0 Patch 4
- Cisco FirePOWER 6.1.0
- Virtual Wireless LAN Controller (vWLC) 8.3.102.0

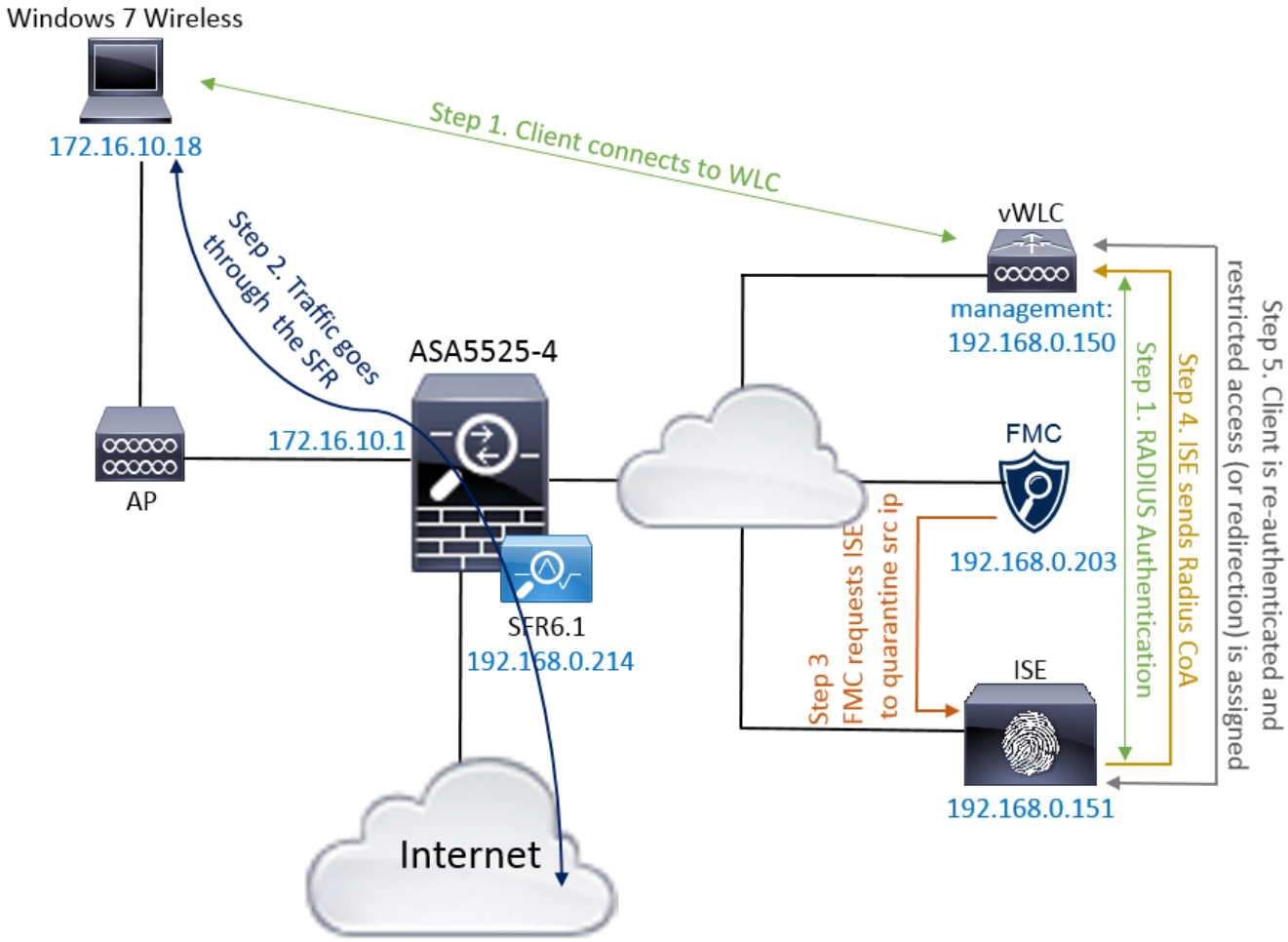
Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konfigurieren

Dieser Artikel behandelt nicht die Erstkonfiguration der ISE-Integration mit FirePOWER, die ISE-Integration mit Active Directory (AD) und die FirePOWER-Integration mit AD. Navigieren Sie für diese Informationen zu Referenzen-Abschnitt. Das FirePOWER 6.1-Sanierungsmodul ermöglicht dem FirePOWER-System die Nutzung von ISE-EPS-Funktionen (Quarantäne, Quarantäne, Port-Herunterfahren) als Problembehebung, wenn eine Korrelationsregel zugeordnet wird.

Hinweis: Für Wireless-Bereitstellungen ist keine Port-Abschaltung verfügbar.

Netzwerkdiagramm



Flussbeschreibung:

1. Ein Client stellt eine Verbindung zu einem Netzwerk her, authentifiziert sich mit der ISE und trifft eine Autorisierungsregel mit einem Autorisierungsprofil, das uneingeschränkten Zugriff auf das Netzwerk gewährt.
2. Der Datenverkehr vom Client fließt dann über ein FirePOWER-Gerät.
3. Der Benutzer startet eine schädliche Aktivität und trifft auf eine Korrelationsregel, die wiederum FirePOWER Management Center (FMC) veranlasst, die ISE-Beseitigung über pxGrid durchzuführen.
4. Die ISE weist dem Endpunkt eine EPSStatus-Quarantäne zu und löst einen RADIUS Change

of Authorization auf ein Netzwerkzugriffsgerät (WLC oder Switch) aus.

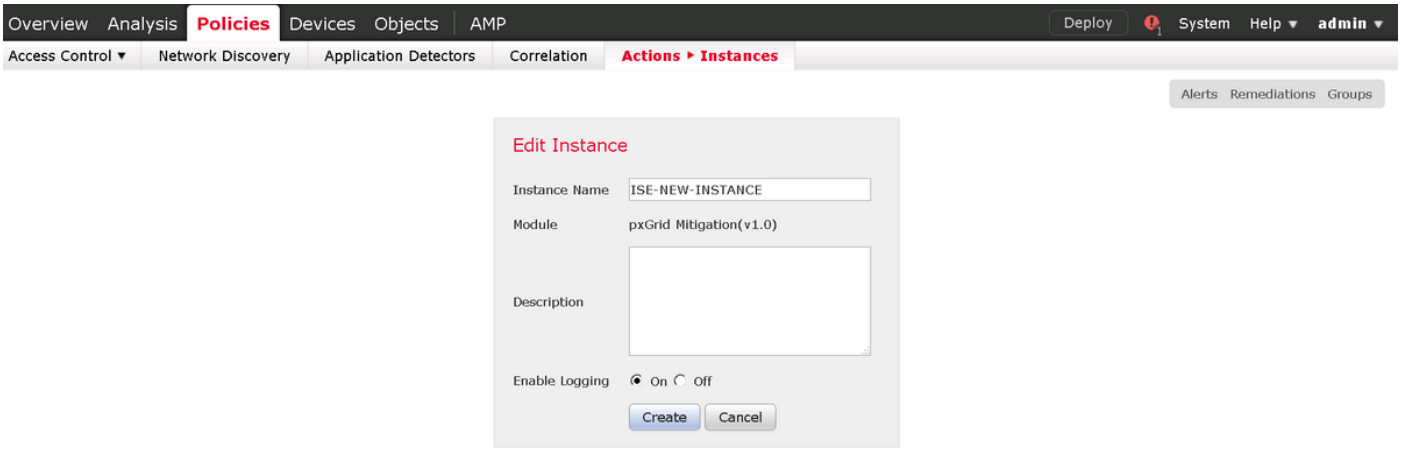
5. Der Client greift auf eine andere Autorisierungsrichtlinie zu, die einen eingeschränkten Zugriff zuweist (ändert SGT oder leitet den SGT an das Portal um oder verweigert den Zugriff).

Hinweis: Network Access Device (NAD) sollte so konfiguriert werden, dass RADIUS Accounting an die ISE gesendet wird, um der ISE IP-Adressinformationen zur Zuordnung der IP-Adresse zu einem Endpunkt bereitzustellen.

Konfigurieren von FirePOWER

Schritt 1: Konfigurieren einer pxGrid-Instanz zur Risikominderung

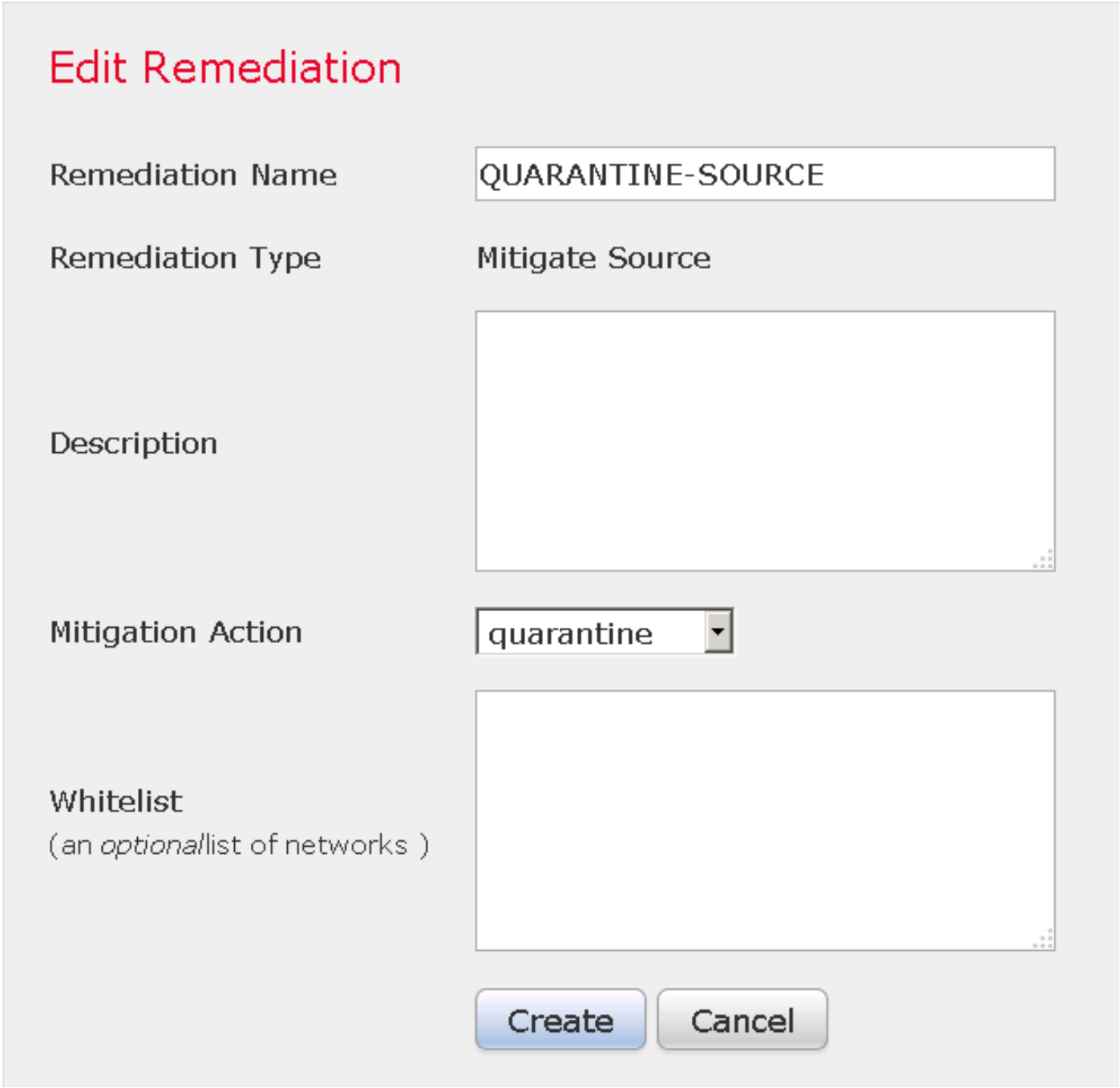
Navigieren Sie zu **Richtlinien > Aktionen > Instanzen**, und fügen Sie pxGrid Mitigation Instance hinzu, wie im Bild gezeigt.



Schritt 2: Konfigurieren Sie eine Problembehebung.

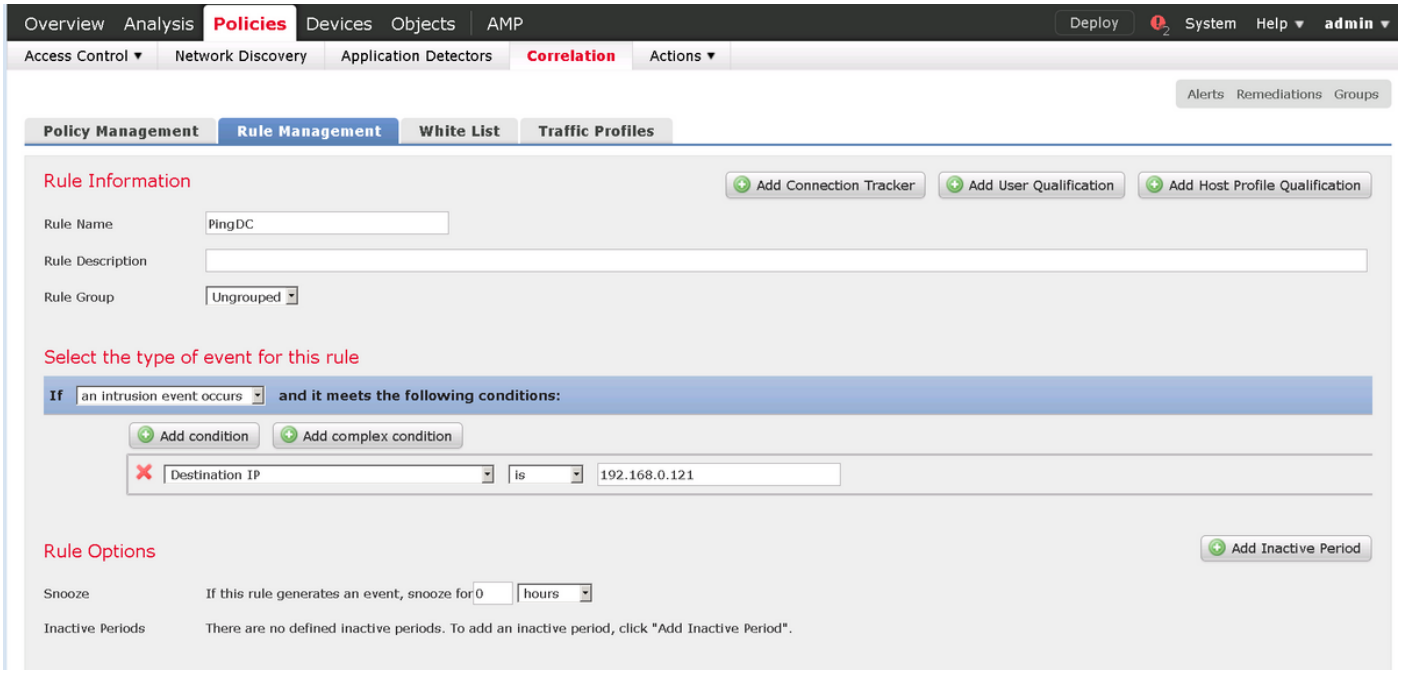
Es stehen zwei Typen zur Verfügung: Ziel minimieren und Quelle minimieren. In diesem Beispiel wird Source Mitigation verwendet. Wählen Sie Sanierungstyp aus, und klicken Sie auf **Hinzufügen**, wie im Bild gezeigt:

Weisen Sie der Problembehebung, wie im Bild gezeigt, eine Aktion zur Problembehebung zu:



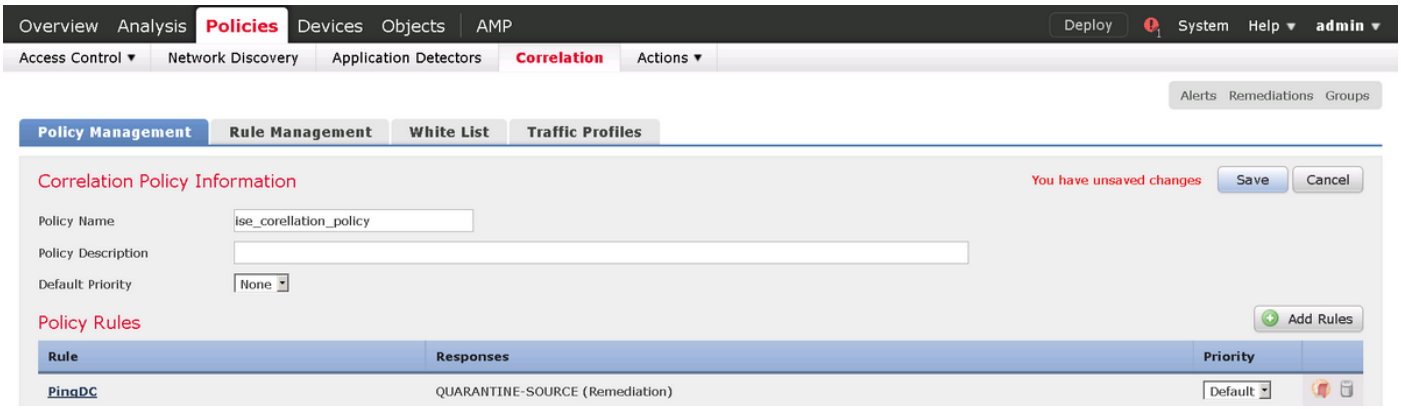
Schritt 3: Konfigurieren einer Korrelationsregel.

Navigieren Sie zu **Policies > Correlation > Rule Management**, und klicken Sie auf **Create Rule Correlation (Regelkorrelation erstellen)**, um die Korrektur auszulösen. Korrelationsregel kann mehrere Bedingungen enthalten. In diesem Beispiel wird Correlation Rule **PingDC** getroffen, wenn ein Angriffsereignis auftritt und die Ziel-IP-Adresse 192.168.0.121 lautet. Für den Test wird eine benutzerdefinierte Intrusion-Regel konfiguriert, die mit der ICMP-Echoantwort übereinstimmt, wie im Bild gezeigt:

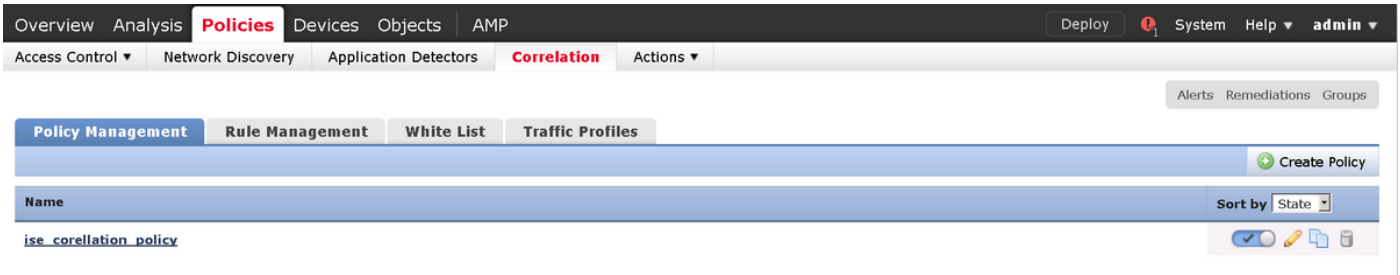


Schritt 4: Konfigurieren einer Korrelationsrichtlinie

Navigieren Sie zu **Richtlinien > Korrelation > Richtlinienmanagement**, und klicken Sie auf **Richtlinie erstellen**, fügen Sie der Richtlinie eine Regel hinzu, und weisen Sie der Richtlinie eine Antwort zu, wie im Bild gezeigt:



Aktivieren Sie die Korrelationsrichtlinie, wie im Bild gezeigt:

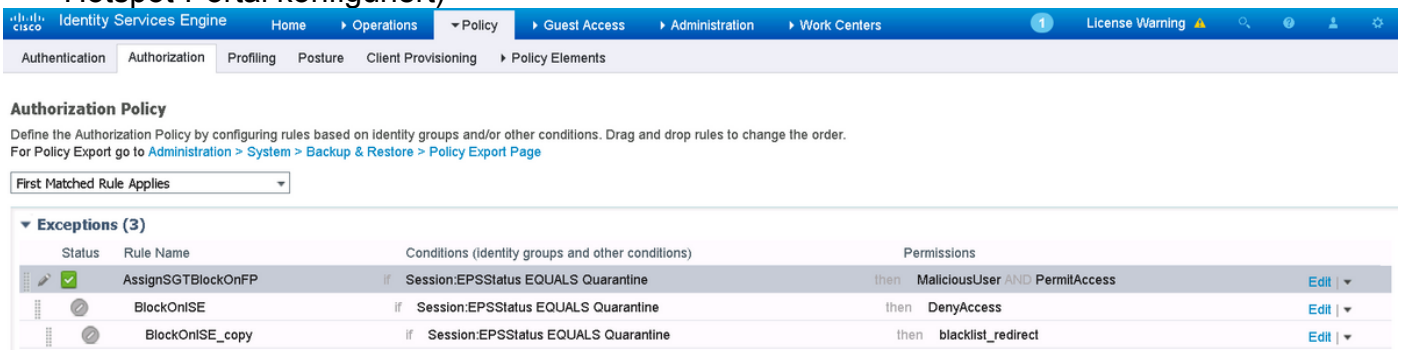


ISE konfigurieren

Schritt 1: Konfigurieren der Autorisierungsrichtlinie

Navigieren Sie zu **Richtlinien > Autorisierung**, und fügen Sie eine neue Autorisierungsrichtlinie hinzu, die nach der Bereinigung aufgerufen wird. **Sitzung** verwenden**: EPSStatus EQUALS Quarantine** als Bedingung. Es gibt mehrere Optionen, die als Ergebnis verwendet werden können:

- Zulassen von Zugriff und Zuweisen eines anderen SGTs (Durchsetzung von Zugriffskontrollbeschränkungen auf Netzwerkgeräten)
- Zugriff verweigern (Benutzer sollte aus dem Netzwerk geworfen werden und nicht wieder eine Verbindung herstellen können)
- Umleitung zu einem **Blacklist**-Portal (in diesem Szenario ist hierfür ein benutzerdefiniertes Hotspot-Portal konfiguriert)

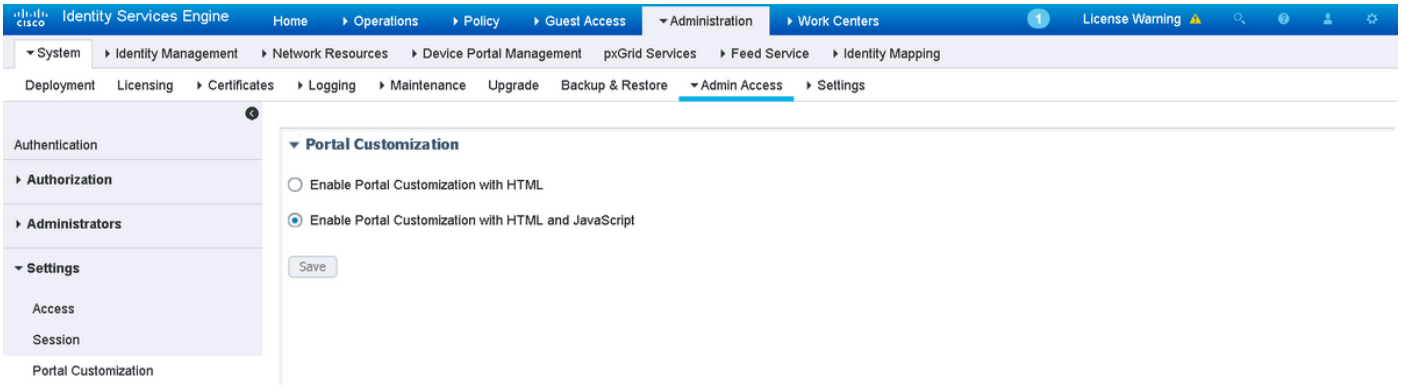


Benutzerdefinierte Portalkonfiguration

In diesem Beispiel wird das Hotspot-Portal als **Blacklist** konfiguriert. Es gibt nur eine Seite mit Richtlinien für akzeptable Nutzung (Acceptable Use Policy, AUP) mit benutzerdefiniertem Text, und es besteht keine Möglichkeit, die AUP zu akzeptieren (dies geschieht mit JavaScript). Um dies zu erreichen, müssen Sie zuerst JavaScript aktivieren und dann einen Code einfügen, der die Schaltfläche und Steuerelemente für die AUP-Anpassung in der Konfiguration der Portalanpassung verbirgt.

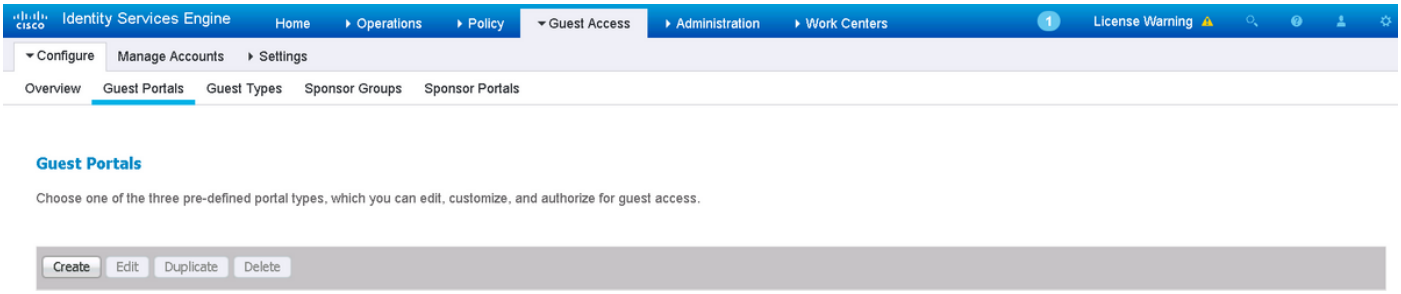
Schritt 1: Aktivieren Sie JavaScript.

Navigieren Sie zu **Administration > System > Admin Access> Settings > Portal Customization.** Wählen Sie **Portal Customization mit HTML und JavaScript aktivieren** und klicken Sie auf **Save**.



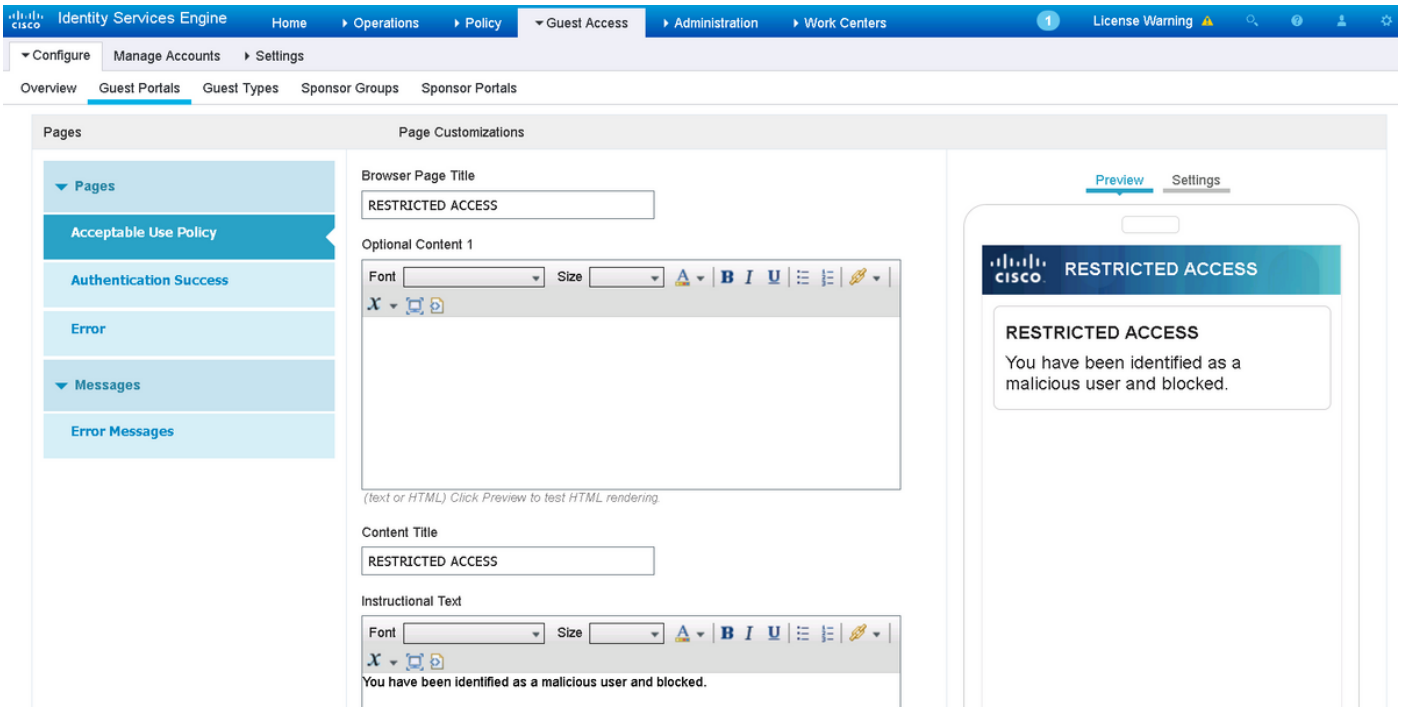
Schritt 2: Erstellen Sie ein Hotspot-Portal.

Navigieren Sie zu **Gastzugriff > Konfigurieren > Gastportale,** und klicken Sie auf **Erstellen**, und wählen Sie dann Hotspot-Typ aus.



Schritt 3: Konfigurieren der Portalanpassung

Navigieren Sie zu **Portalseitenanpassung**, und ändern Sie Titel und Inhalt, um dem Benutzer eine entsprechende Warnung zu geben.



Navigieren Sie zu **Option Content 2**, klicken Sie auf **HTML-Quelle umschalten**, und fügen Sie das Skript in Folgendes ein:

Klicken Sie auf **HTML-Quelle deaktivieren.**

Optional Content 2

Font Size

```
<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>
<br _moz_editor_bogus_node="TRUE" />
```

(text or HTML) Click Preview to test HTML rendering.

Überprüfen

Verwenden Sie die Informationen in diesem Abschnitt, um zu überprüfen, ob Ihre Konfiguration ordnungsgemäß funktioniert.

FirePOWER

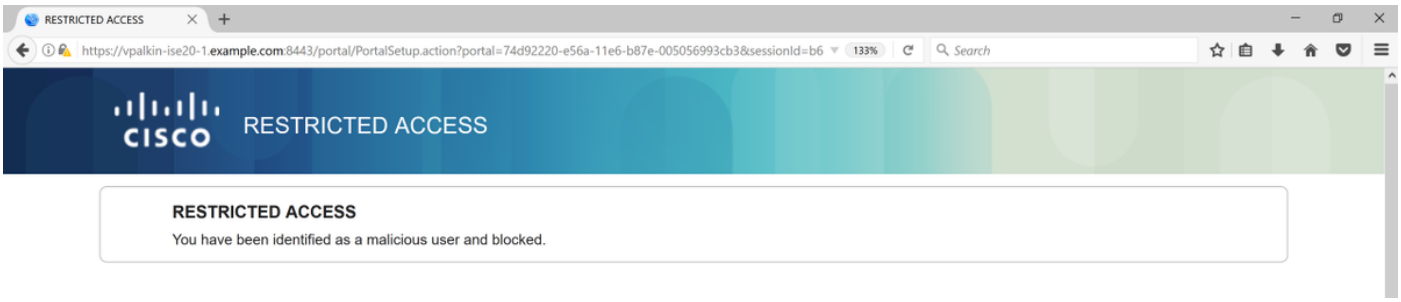
Der Auslöser für die Problembehebung ist ein Treffer von Korrelationsrichtlinien/-regeln. Navigieren Sie zu **Analyse > Correlation > Correlation > Correlation Events**, und überprüfen Sie, ob ein Korrelationsereignis aufgetreten ist.

ISE

Die ISE sollte dann Radius auslösen: CoA und erneute Authentifizierung des Benutzers. Diese Ereignisse können unter **Operation > RADIUS Livelog** verifiziert werden.

In diesem Beispiel hat die ISE dem Endpunkt verschiedene SGT **MaliciousUser** zugewiesen. Im Falle eines **Deny Access** Authorization-Profils verliert der Benutzer die Wireless-Verbindung und kann keine Verbindung mehr herstellen.

Die Sanierung durch ein Blacklist-Portal. Wenn eine Behebungs-Autorisierungsregel für die Umleitung zum Portal konfiguriert ist, sollte sie aus Angreifersicht wie folgt aussehen:



Fehlerbehebung

Dieser Abschnitt enthält Informationen, die Sie zur Fehlerbehebung bei Ihrer Konfiguration verwenden können.

Navigieren Sie zu **Analyse > Korrelation > Status** wie in diesem Bild gezeigt.

Die Ergebnismeldung sollte entweder **Erfolgreiche Beendigung der Problembehebung** oder eine bestimmte Fehlermeldung zurückgeben. Syslog überprüfen: **System > Monitoring > Syslog** und Filter Output with **pxgrid**. Die gleichen Protokolle können in **/var/log/messages** überprüft werden.

Zugehörige Informationen

- 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