Firepower 6.1 pxGrid-verbetering met ISE configureren

Inhoud

Inleiding

Dit document beschrijft hoe u Firepower 6.1 pxGrid Design kunt configureren met Identity Services Engine (ISE). Firepower 6.1+ ISE-servicemodule kan met ISE Endpoint Protection Service (EPS) worden gebruikt voor de automatisering van qurantine/chantage van aanvallers op de netwerktoegangslaag.

Voorwaarden

Vereisten

Cisco raadt u aan basiskennis van deze onderwerpen te hebben:

- Cisco ISE
- Cisco FireSIGHT

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco ISE versie 2.0 Patch 4
- Cisco Firepower 6.1.0
- Virtual Wireless LAN-controller (vWLC) 8.3.102.0

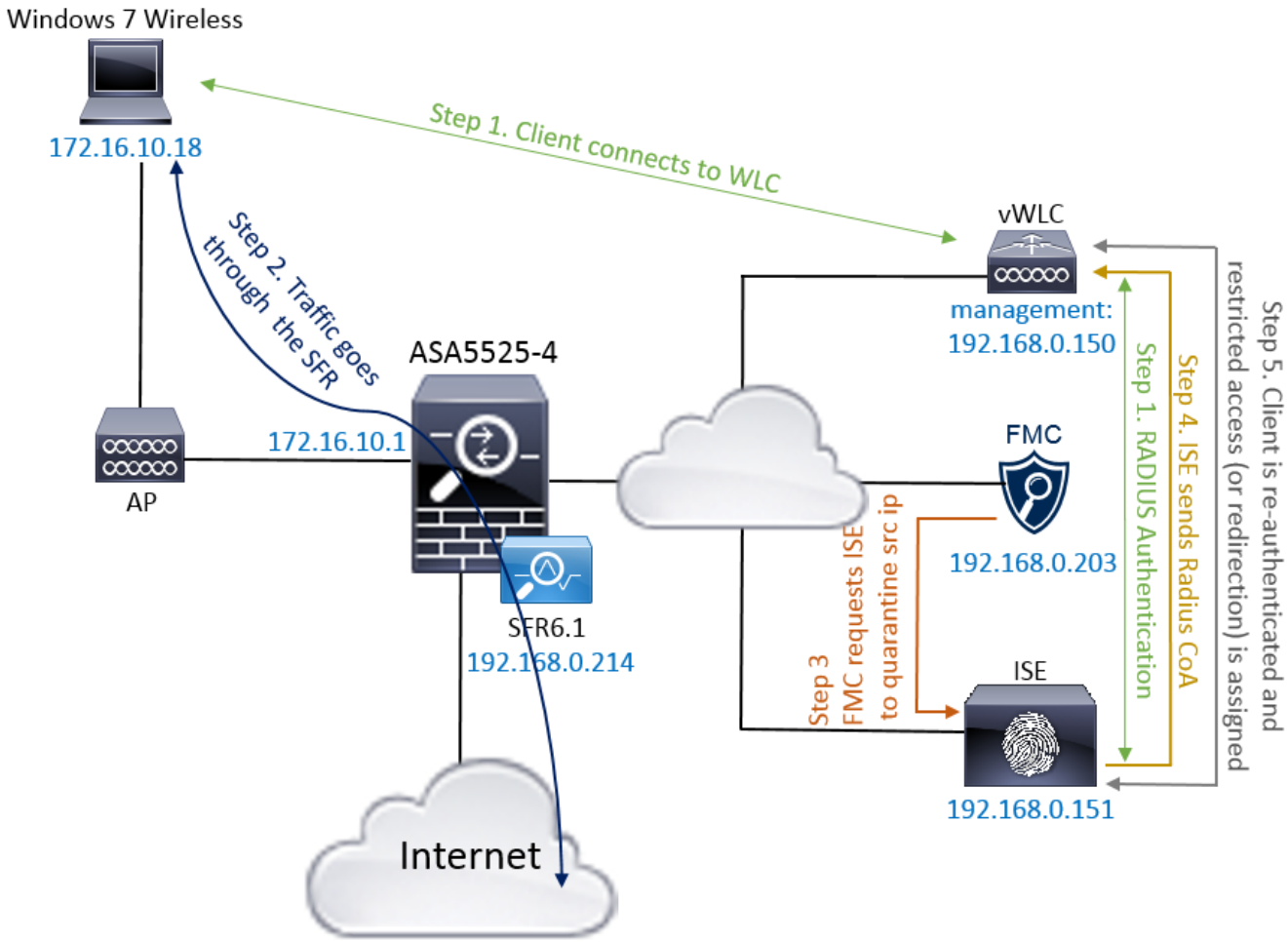
De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Configureren

Dit artikel heeft geen betrekking op de eerste configuratie van ISE-integratie met Firepower, ISE-integratie met Active Directory (AD), Firepower integration met AD. navigeer voor deze informatie naar het gedeelte referenties. Firepower 6.1 Remediation-module stelt het brandweersysteem in staat om ISE EPS-functies (quarantaine, niet-quarantaine, sluiting van poorten) te gebruiken als een oplossing wanneer correlatieregel wordt geneutraliseerd.

> Opmerking: Poortsluiting is niet beschikbaar voor draadloze implementaties.

Netwerkdiagram



De stroombeschrijving:

1. Een cliënt verbindt zich met een netwerk, verklaart zich authentiek met ISE en slaat een machtigingsregel in met een vergunningsprofiel dat onbeperkte toegang tot het netwerk verleent.
2. Het verkeer van de cliënt stroomt dan door een apparaat van de vuurkracht.
3. Gebruiker begint een kwaadaardige activiteit uit te voeren en slaat een correlatieregel in die op zijn beurt Firepower Management Center (FMC) geactiveerd om ISE-herstel uit te voeren via pxGrid.
4. ISE wijst een EPSStatus Quarantine aan het eindpunt toe en brengt RADIUS-wijziging van

autorisatie op een netwerk access apparaat (WLC of Switch) in werking.

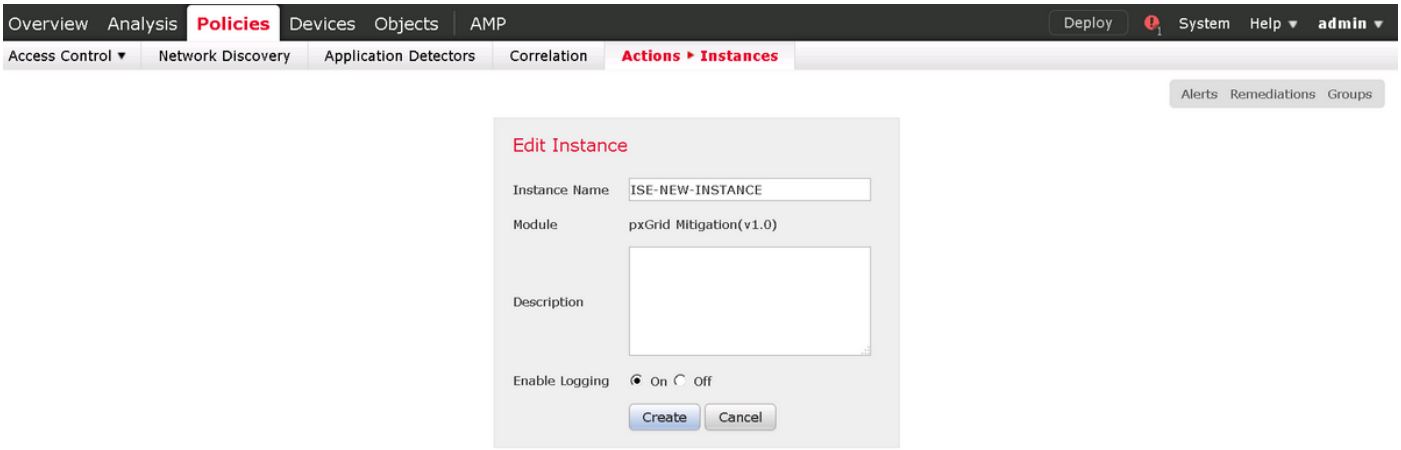
5. De cliënt treft een ander vergunningsbeleid dat een beperkte toegang toekent (wijzigt SGT of omwijst naar portal of ontkent toegang).

Opmerking: Network Access Devices (NAD) moet worden geconfigureerd om RADIUS-accounting naar ISE te verzenden om deze te voorzien van ip-adresinformatie die wordt gebruikt om IP-adres naar een eindpunt in te delen.

Firepower instellen

Stap 1. Configureer een pGrid-limiteringsinstantie.

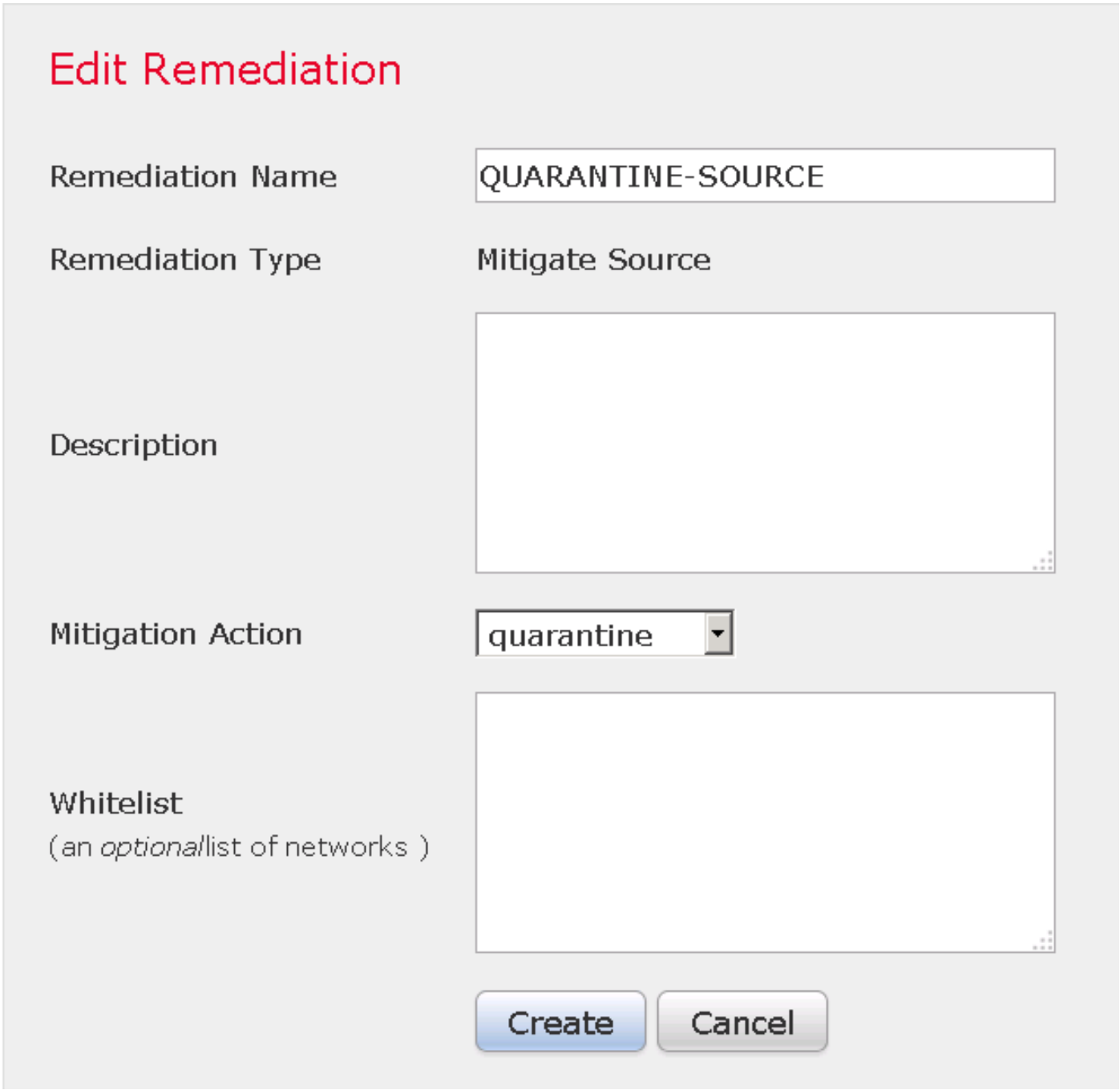
Navigeer naar **beleid > Handelingen > Instellingen** en voeg de instantie voor de beperking van de penis toe zoals in de afbeelding.



Stap 2. Configureer een correctie.

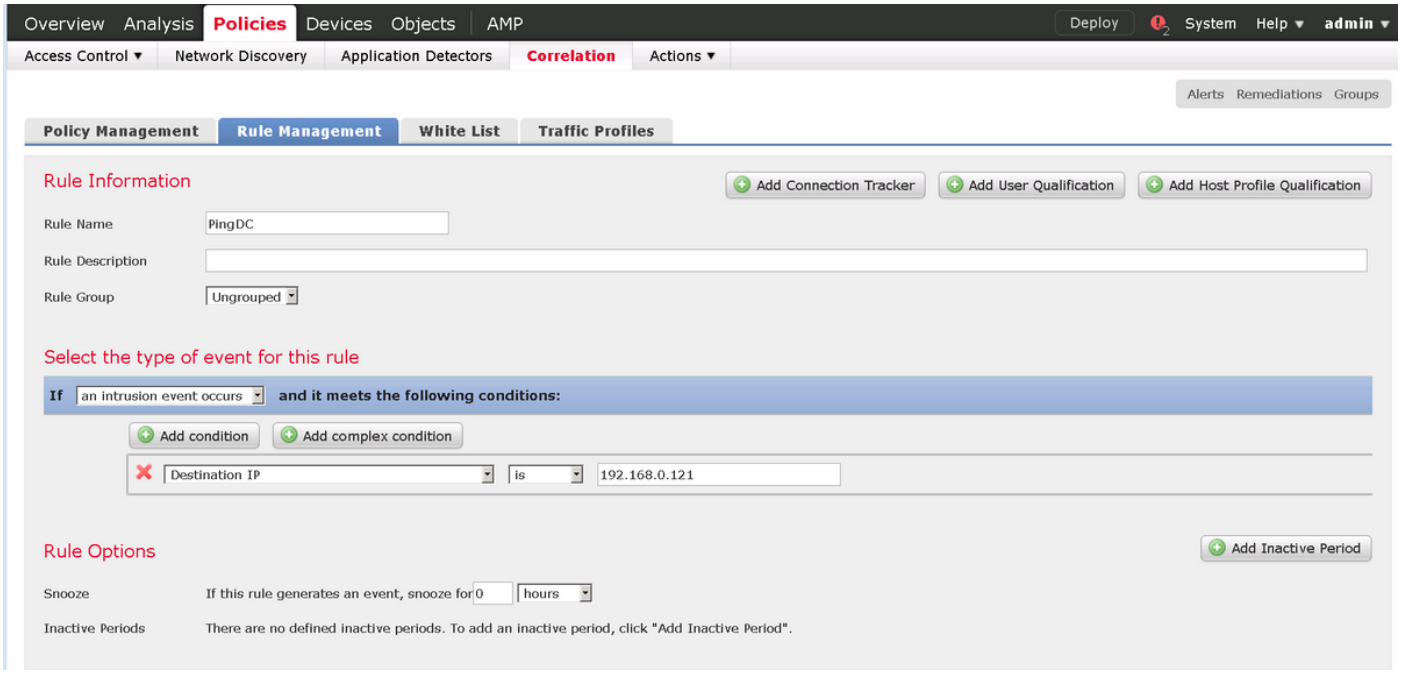
Er zijn twee soorten beschikbaar: Bestemming verminderen en Bron verzachten. In dit voorbeeld wordt bronbeperking gebruikt. Kies het hersteltype en klik op **Toevoegen** zoals in de afbeelding:

Wijzig actie voor beperking aan de aanpassing toe zoals in de afbeelding:



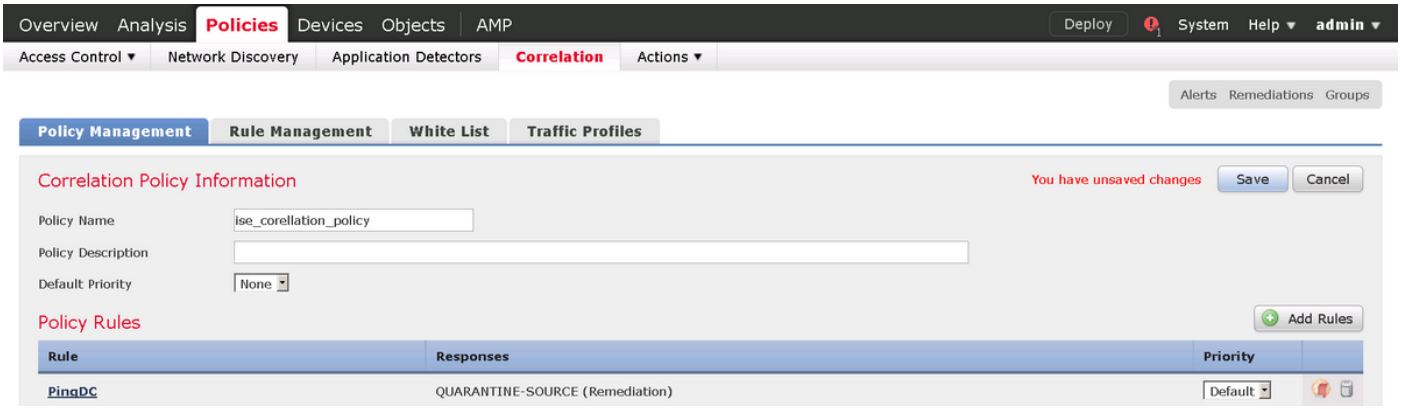
Stap 3. Configureer een correlatieregel.

Navigeer naar **beleid > Correlatie > Regelbeheer** en klik op **Regel** correlatieregel maken is de aanzet tot herstel. De correlatieregel kan meerdere voorwaarden bevatten. In dit voorbeeld wordt **PingDC** van de correlatieregel geraakt als er een inbraakgebeurtenis optreedt en het IP-adres van de bestemming 192.168.0.121 is. Aangepaste inbraakregel die een weerwoord van de icmp weergeeft, wordt ingesteld voor het doel van de test zoals in de afbeelding wordt getoond:

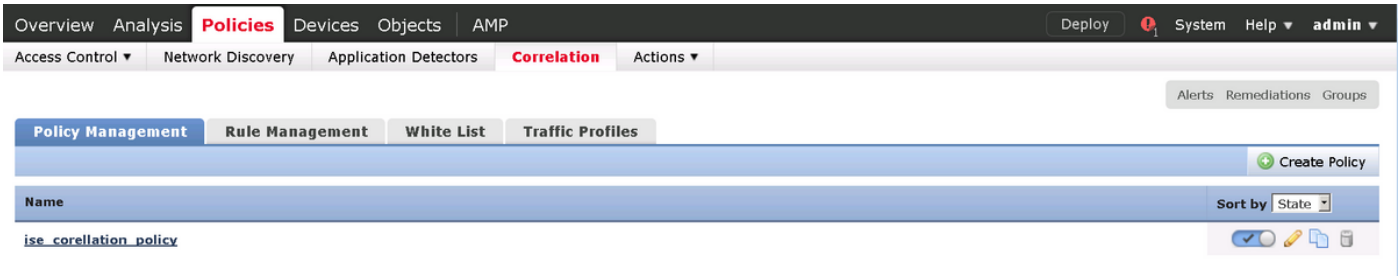


Stap 4. Een correlatiebeleid configureren.

Navigeer naar **beleid > Correlatie > Beleidsbeheer** en klik op **Beleidsbeleid maken**, voeg regel aan het beleid toe en geef antwoord aan zoals in de afbeelding:



Schakel het correlatiebeleid in zoals in de afbeelding:

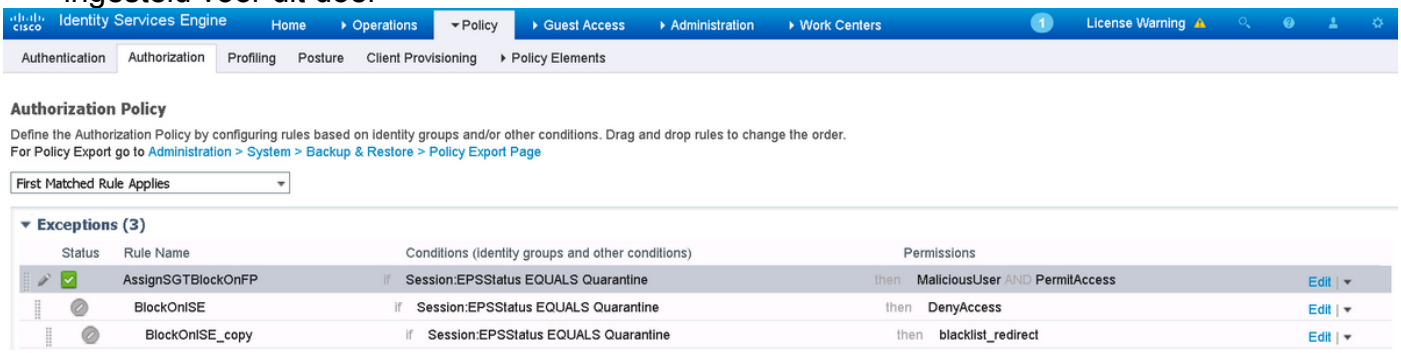


ISE configureren

Stap 1. Het machtigingsbeleid configureren.

Navigeer naar **Beleidsbeleid > Vergunning** en voeg een nieuw vergunningsbeleid toe dat zal worden aangetast nadat de verlossing heeft plaatsgevonden. **Sessie** gebruiken**: EPStatus EQUALS Quarantine** als de aandoening. Er zijn verschillende opties die als gevolg daarvan kunnen worden gebruikt:

- Toegang verlenen en een ander SGT toewijzen (afdwingen toegangscontrole beperking op netwerkapparaten)
- Deny Access (de gebruiker moet uit het netwerk worden gezet en kan niet opnieuw verbinden)
- Omleiden naar een **zwarte lijst** portal (in dit scenario is een aangepaste hotspot portal ingesteld voor dit doel

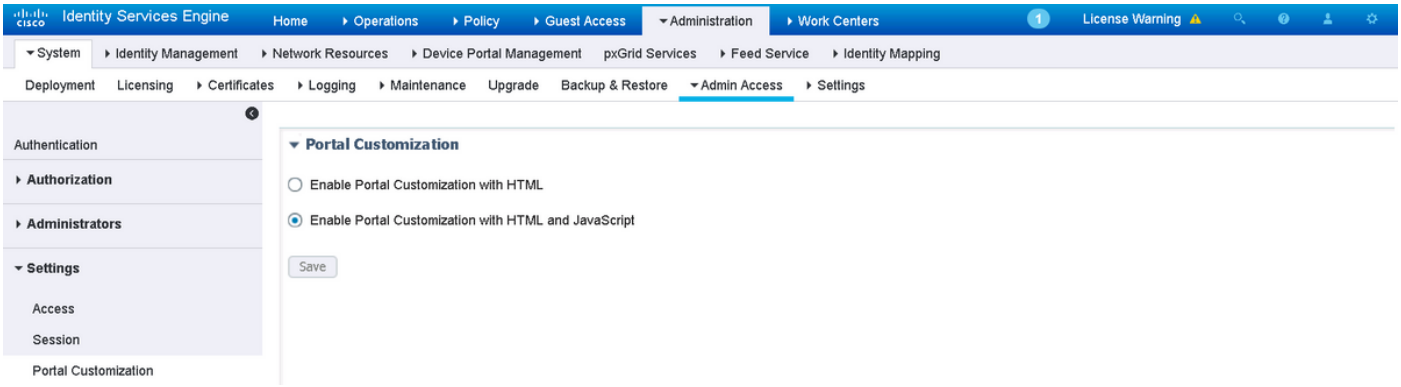


Aangepaste poortconfiguratie

In dit voorbeeld wordt de hotspot portal ingesteld als een **zwarte lijst**. Er is alleen een pagina Acceptable use Policy (AUP) met aangepaste tekst en er is geen mogelijkheid om de AUP (dit wordt gedaan met JavaScript) te aanvaarden. Om dit te bereiken, moet u eerst JavaScript inschakelen en dan een code kleven die de AUP-knop verbergt en in de configuratie van de portal regelt.

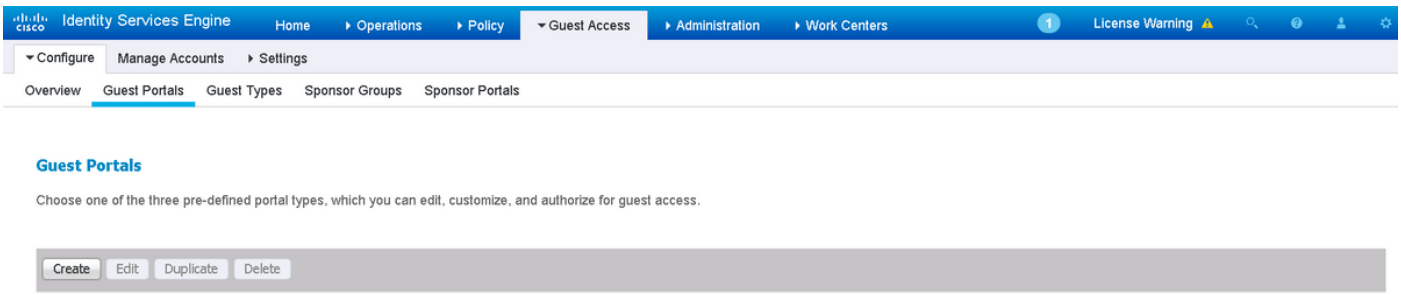
Stap 1. Schakel JavaScript in.

Navigeer naar **Beheer > Systeem > Admin Access> Instellingen > Portal Aanpassen.** Kies **Portal customization met HTML en JavaScript** en klik op **Opslaan**.



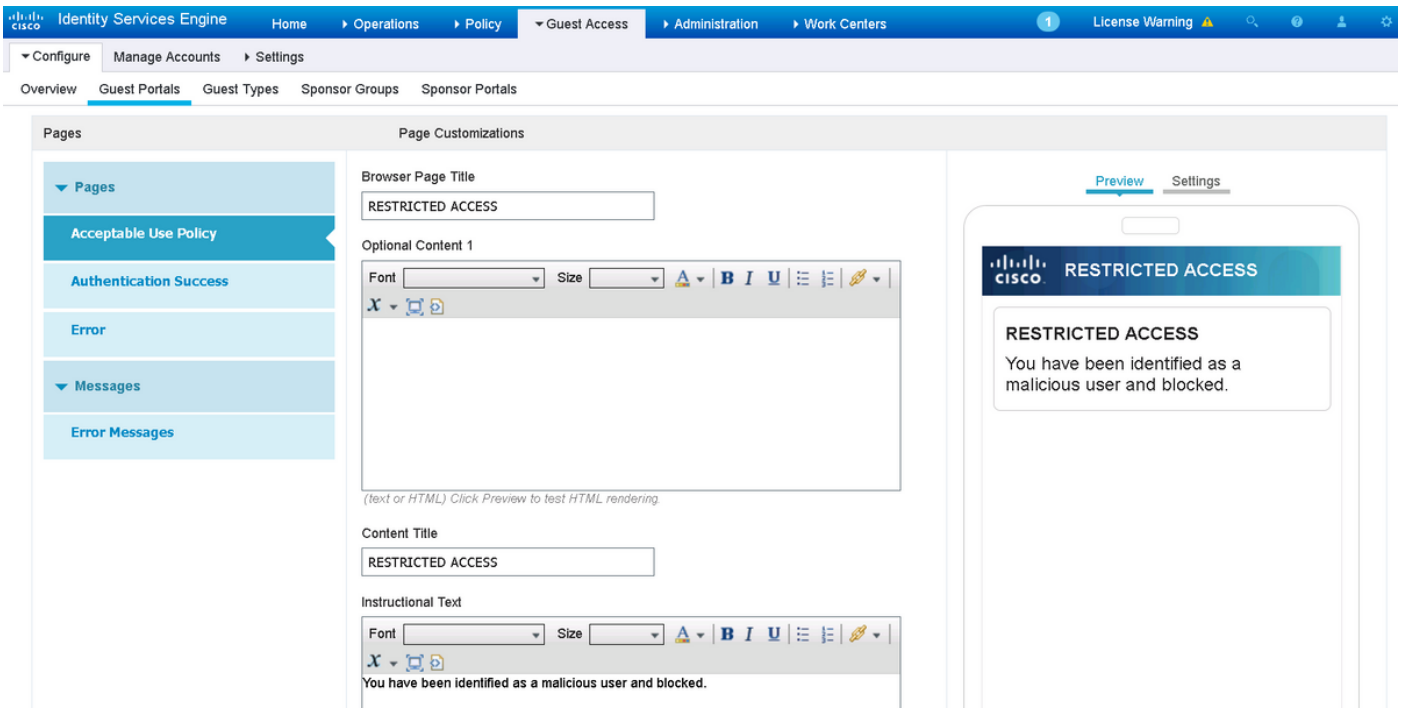
Stap 2. Maak een hotspotportal.

Navigeer om **toegang te bestellen > Portals bestellen > Beelden instellen** en klik op **Maken** en kies dan Hotspot type.



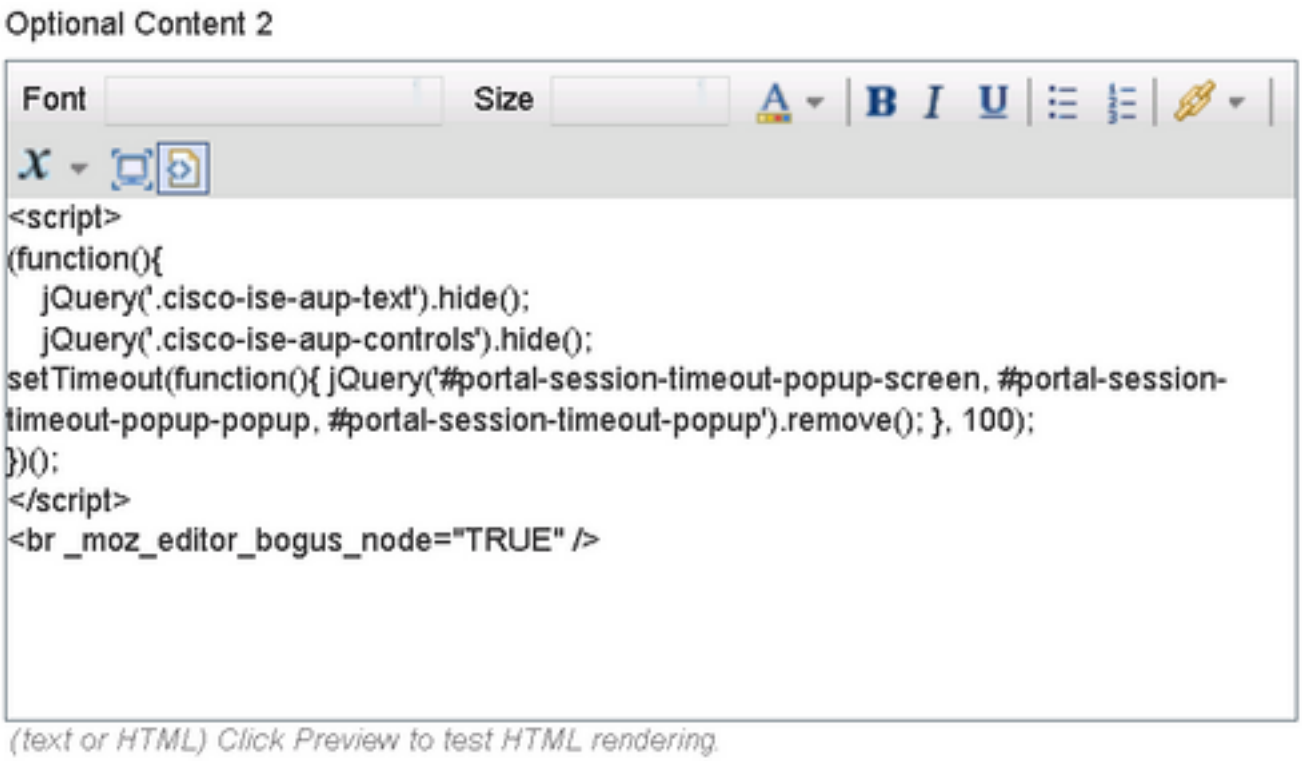
Stap 3. Configureer portal voor aanpassing.

Navigeer naar **Portal Page Aanpassen** en verander titels en inhoud om de gebruiker een juiste waarschuwing te geven.



Scrolt naar **Optie Content 2**, klik op **Google HTML Source** en plak het script binnen:

Klik op **HTML-bron los.**



Verifiëren

Gebruik de informatie in deze sectie om te controleren of uw configuratie correct werkt.

vuurkracht

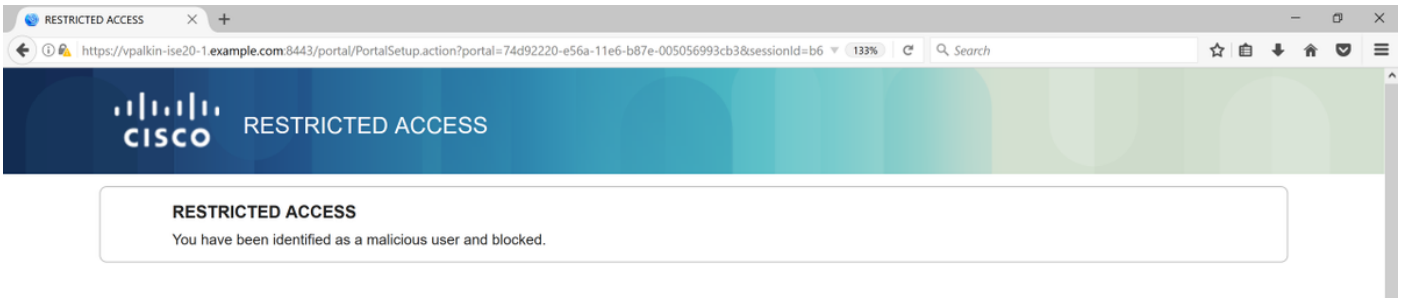
Een poging om iets aan dit probleem te doen is gebaseerd op een correlatie beleid/regelgeving. Navigeer naar **Analyse > Correlatie > Correlatie gebeurtenissen** en controleer of er een correlatie is geweest.

ISE

ISE moet dan Radius activeren: CoA en reauthentiek de gebruiker, deze gebeurtenissen kunnen in **Handeling > RADIUS Livellog** worden geverifieerd.

In dit voorbeeld, heeft ISE verschillende SGT **Malicious User** aan het eindpunt toegewezen. In het geval van het autorisatieprofiel van de **Deny Access**, verliest de gebruiker de draadloze verbinding en kan hij geen verbinding meer maken.

Het herstel met een zwarte lijst portal Als de regel voor het verlenen van een vergunning voor het herstel is ingesteld om naar het portal te gaan, zou deze er uit het oogpunt van de aanvaller zo moeten uitzien:



Problemen oplossen

Deze sectie verschaft informatie die u kunt gebruiken om problemen met uw configuratie op te lossen.

Navigeer naar **Analyse > Correlatie > Status** zoals in deze afbeelding.

Resultaat-bericht moet ofwel **Voltooien van het herstel met succes** of een bepaalde foutmelding retourneren. Controleer het woordenboek: **Systeem > Controle > SYS** en filter uitvoer met **pxgrid**. Dezelfde logbestanden kunnen ook worden geverifieerd in **/var/log/messen.**

Gerelateerde informatie

- 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