Stappen voor configuratie van FireSIGHT-systemen

Inhoud

Inleiding

Nadat u een FireSIGHT Management Center of een FirePOWER-apparaat hebt gereinigd, dient u verschillende stappen te ondernemen om het systeem volledig functioneel te maken en waarschuwingen te genereren voor inbraakgebeurtenissen; zoals het installeren van licenties, het registreren van de apparatuur, het toepassen van gezondheidsbeleid, systeembeleid, toegangscontrolebeleid, inbraakbeleid enz. Dit document is een aanvulling op de FireSIGHT System Installatie Guide.

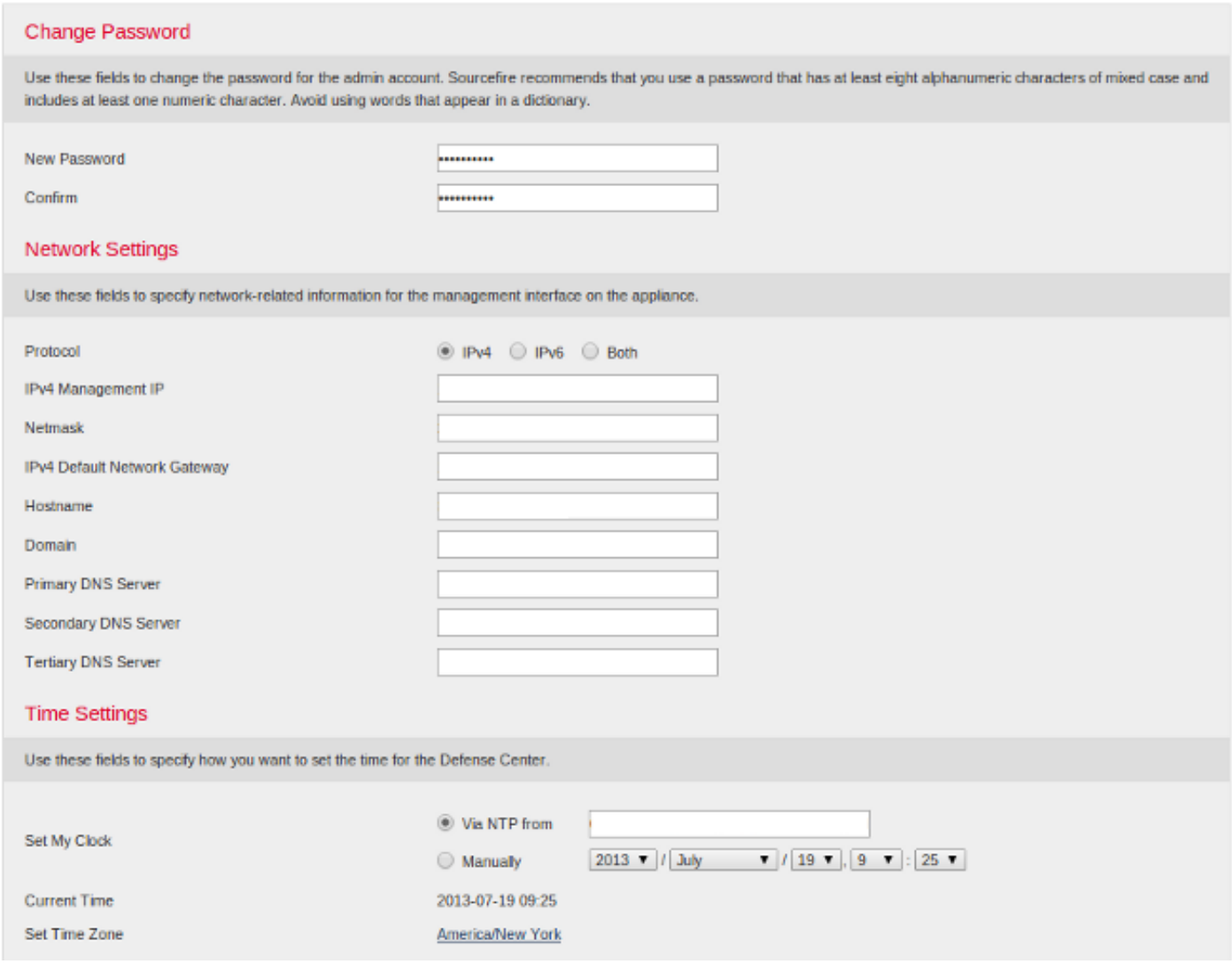
Voorwaarden

Deze handleiding gaat ervan uit dat u de FireSIGHT System Installatie Guide zorgvuldig hebt gelezen.

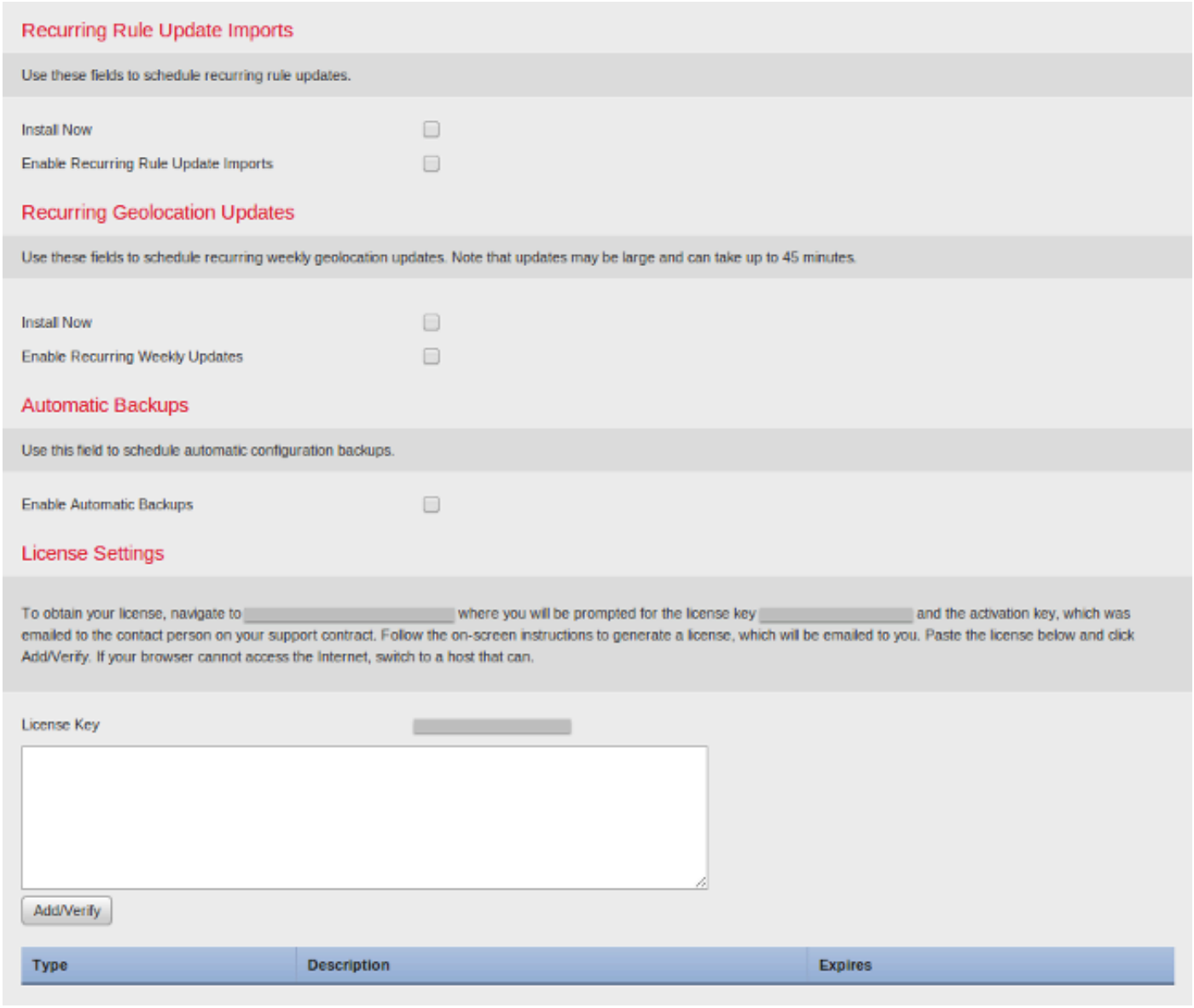
Configuratie

Stap 1: Eerste instelling

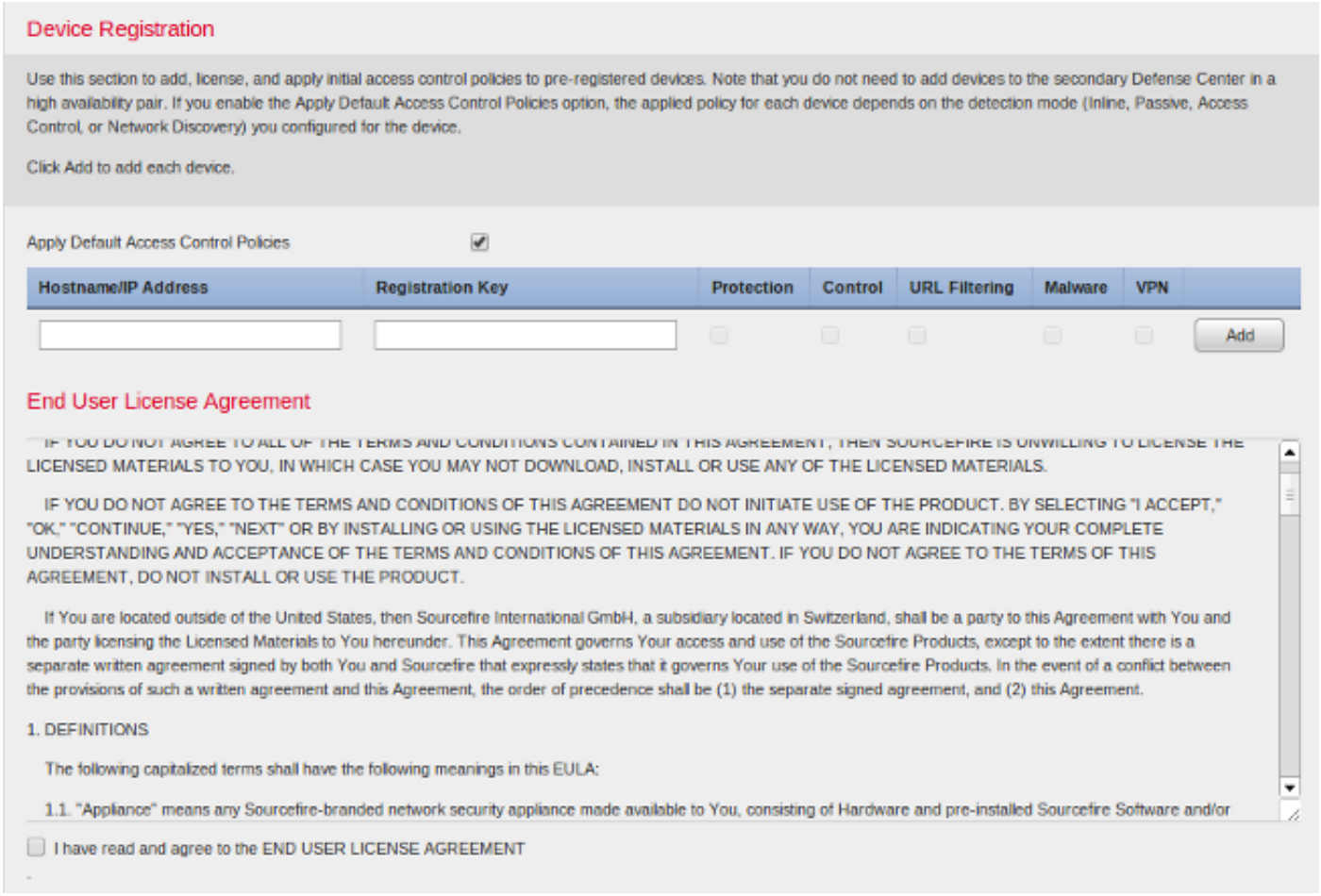
Op uw FireSIGHT Management Center moet u het installatieproces voltooien door in de webinterface te loggen en de eerste configuratieopties in de setup-pagina te specificeren, die hieronder wordt weergegeven. Op deze pagina moet u het beheerwachtwoord wijzigen en kunt u ook netwerkinstellingen instellen zoals Domain en DNS-servers en de tijdconfiguratie instellen.



U kunt optioneel terugkerende regel en geolocation updates evenals automatische back-ups configureren. Alle functiekaarten kunnen ook op dit punt worden geïnstalleerd.



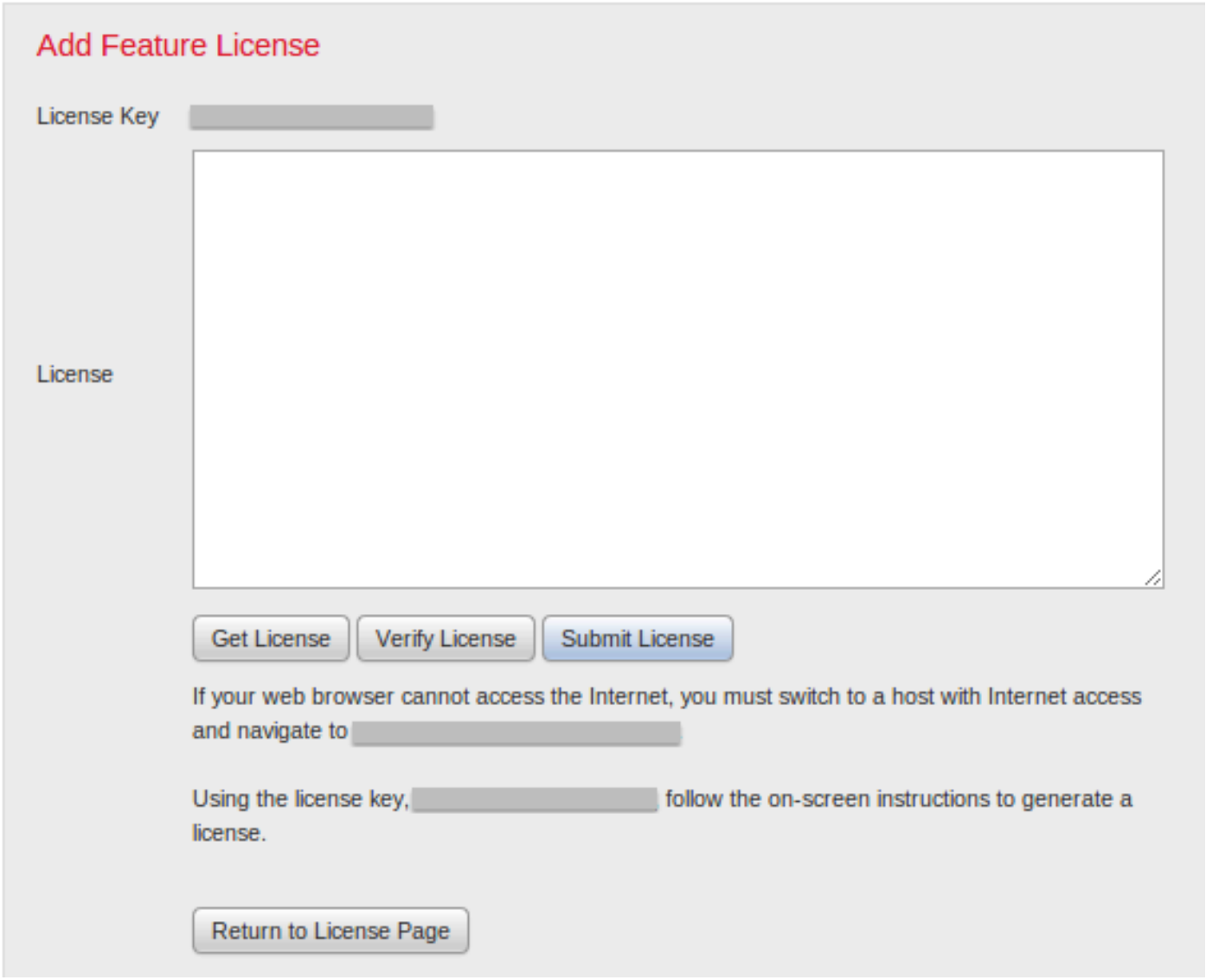
Op deze pagina kunt u een apparaat ook registreren in het FireSIGHT Management Center en een detectiemodus instellen. De detectie modus en andere opties die u tijdens de registratie kiest, bepalen de standaardinterfaces, inline sets en zones die het systeem maakt, evenals het beleid dat het eerst op beheerde apparaten van toepassing is.



Stap 2: Installeer licenties

Als u tijdens de eerste setup-pagina geen licenties hebt geïnstalleerd, kunt u de taak als volgt voltooien:

- Navigeren naar de volgende pagina: **Systeem > Licenties**.
- Klik op **Nieuwe licentie toevoegen**.



Als u geen licentie hebt ontvangen, neemt u contact op met de vertegenwoordiger van uw account.

Stap 3: Het systeembeleid toepassen

Het systeembeleid specificeert de configuratie voor verificatieprofielen en tijdsynchronisatie tussen het FireSIGHT Management Center en de beheerde apparaten. Om het systeembeleid te configureren of toe te passen, navigeer het **systeem > Local > System Policy**. Een standaardsysteembeleid wordt geleverd, maar moet worden toegepast op alle beheerde apparaten.

Stap 4: Het gezondheidsbeleid toepassen

Het gezondheidsbeleid wordt gebruikt om te configureren hoe beheerde apparaten hun gezondheidstoestand rapporteren aan het FireSIGHT Management Center. Om het gezondheidsbeleid te configureren of toe te passen, dient u te **navigeren** naar **Gezondheid > Gezondheidsbeleid**. Er is een standaard gezondheidsbeleid voorzien, maar dat moet worden toegepast op alle beheerde apparaten.

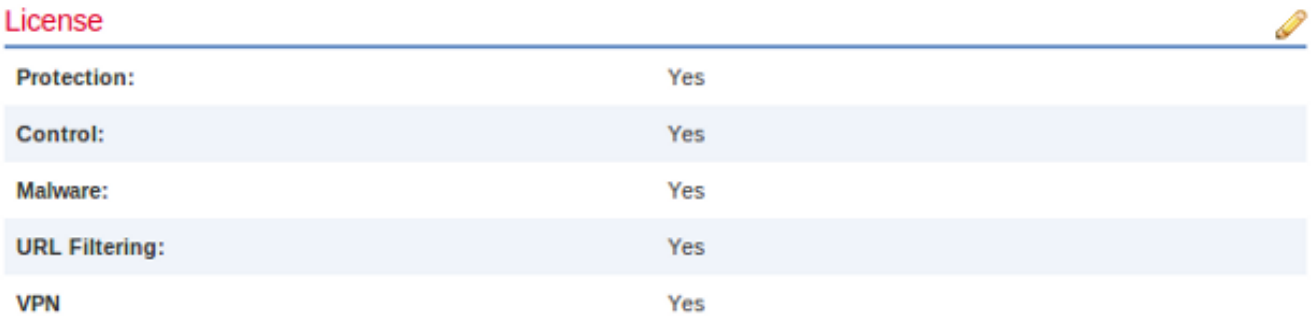
Stap 5: Beheerde apparaten registreren

Als u apparaten tijdens de eerste setup-pagina niet hebt geregistreerd, raadpleegt u dit document voor instructies voor het registreren van een apparaat in een FireSIGHT Management Center.

Stap 6: Geïnstalleerde licenties inschakelen

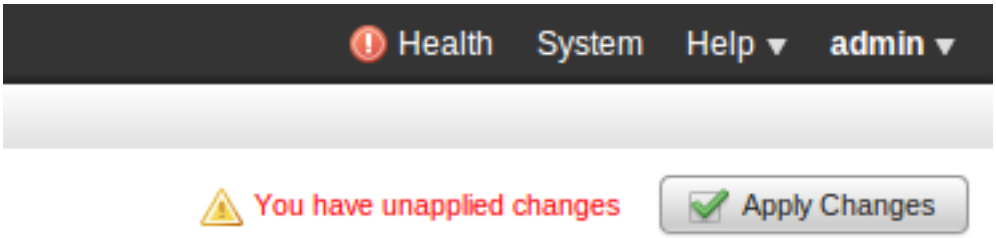
Voordat u een functielicentie op uw apparaat kunt gebruiken, moet u dit voor elk beheerd apparaat inschakelen.

1. Navigeren naar de volgende pagina: **Apparaten > Apparaatbeheer**.
2. Klik op het apparaat waarvoor u de licenties wilt activeren en voer het tabblad Apparaat in.
3. Klik op het pictogram **Bewerken** (*potlood*) naast Licentie.



Schakel de gewenste licenties voor dit apparaat in en klik op **Opslaan**.

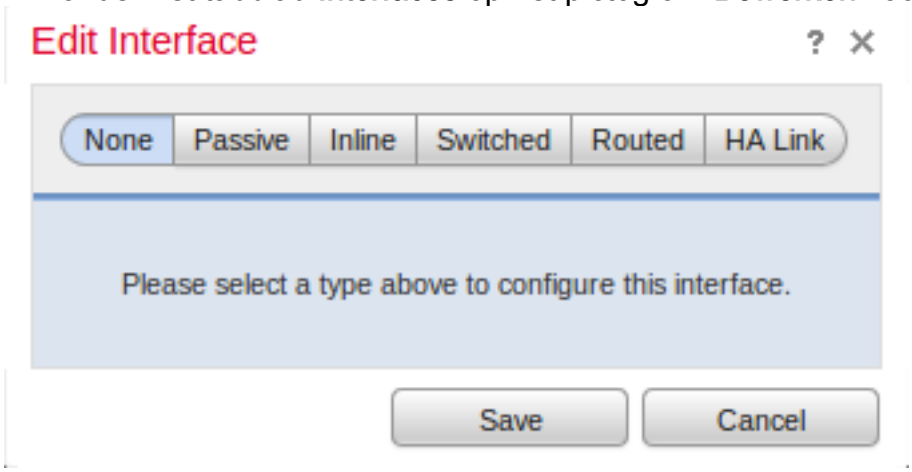
Merk op dat het bericht "*U hebt de wijzigingen niet toegepast*" in de rechterbovenhoek staat. Deze waarschuwing blijft actief, zelfs als u niet op de pagina voor apparaatbeheer klikt totdat u op de knop **Wijzigingen toepassen** klikt.



Stap 7: Gebiedsinterfaces configureren

1. Navigeer naar de volgende pagina-**apparaten > Apparaatbeheer**.
2. Klik op het pictogram **Bewerken** (potlood) voor de sensor van uw keuze.

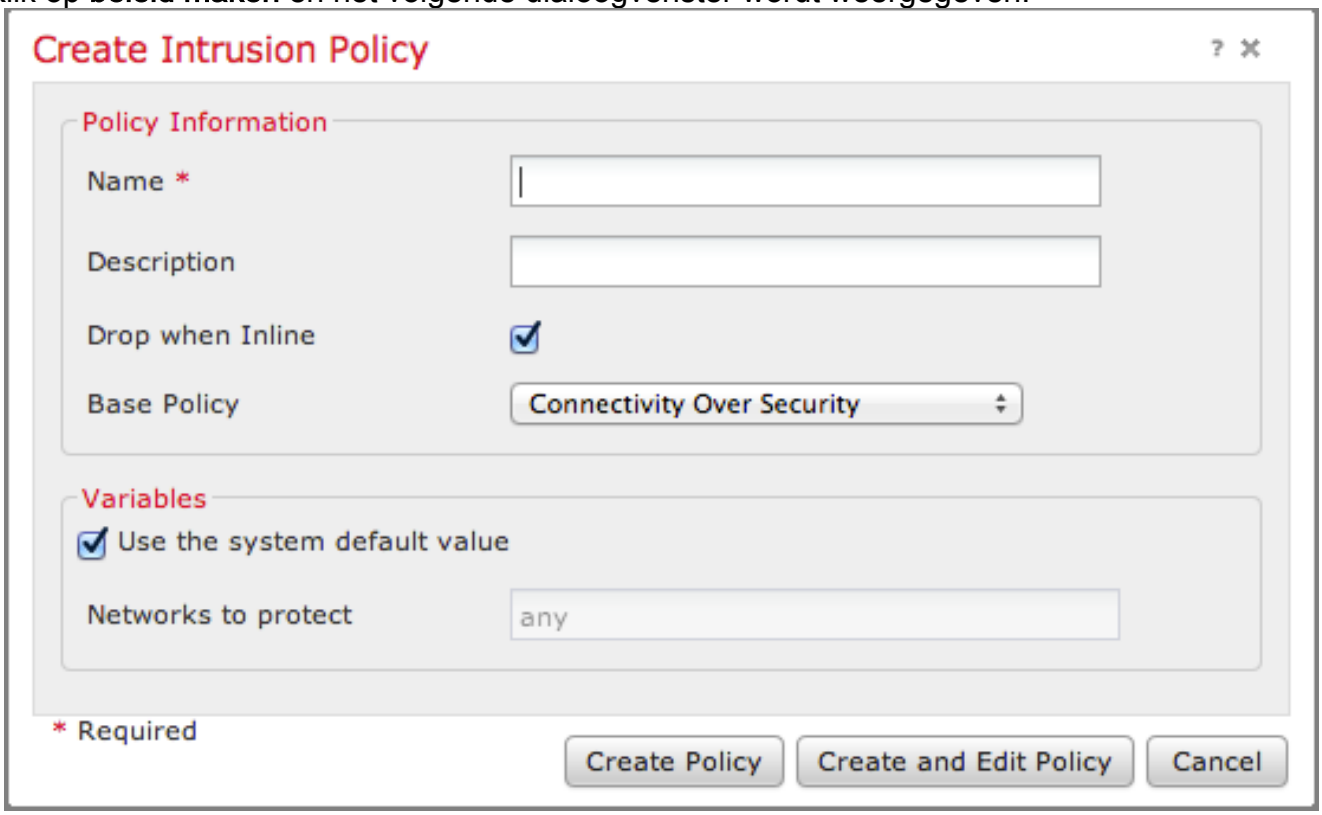
3. Klik onder het tabblad **Interfaces** op het pictogram **Bewerken** voor de interface van uw keuze.



Selecteer een passieve of inline interfaceconconfiguratie. Switched en Routed interfaces vallen buiten het toepassingsgebied van dit artikel.

Stap 8: Het inbraakbeleid configureren

- Navigeer naar de volgende pagina: **Beleid > Inbraakbeleid > Inbraakbeleid.**
- Klik op **beleid maken** en het volgende dialoogvenster wordt weergegeven:



U moet een naam toewijzen en het te gebruiken basisbeleid definiëren. Afhankelijk van uw plaatsing kunt u ervoor kiezen om de optie **Daling** te hebben **wanneer Inline** ingeschakeld. Defineert de netwerken die u wilt beveiligen om valse positieven te verminderen en de prestaties van het systeem te verbeteren.

Als u op **beleid maken** klikt, worden uw instellingen opgeslagen en wordt het IPS-beleid gemaakt.

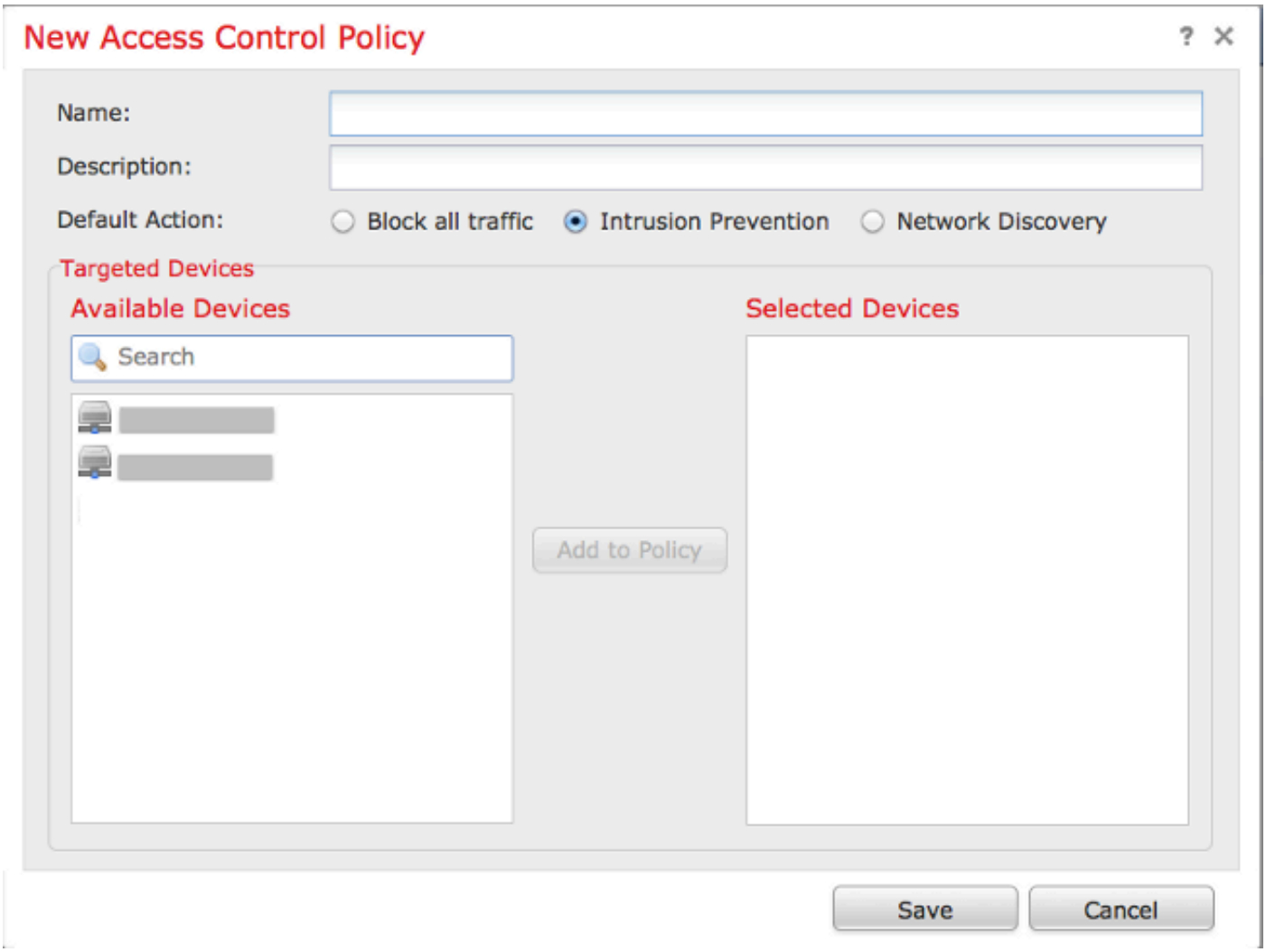
Als u wijzigingen in het inbraakbeleid wilt aanbrengen, kunt u in de plaats **Beleid maken en bewerken**.

> Opmerking: Inbraakbeleid wordt toegepast als onderdeel van het beleid inzake toegangscontrole. Nadat een inbraakbeleid is toegepast, kunnen alle wijzigingen worden toegepast zonder het gehele beleid voor toegangscontrole opnieuw toe te passen door op de knop **Opnieuw** te klikken.

Stap 9: Een toegangscontrolebeleid instellen en toepassen

1. Navigeer naar **beleid > Toegangsbeheer**.

2. Klik op **Nieuw beleid**.

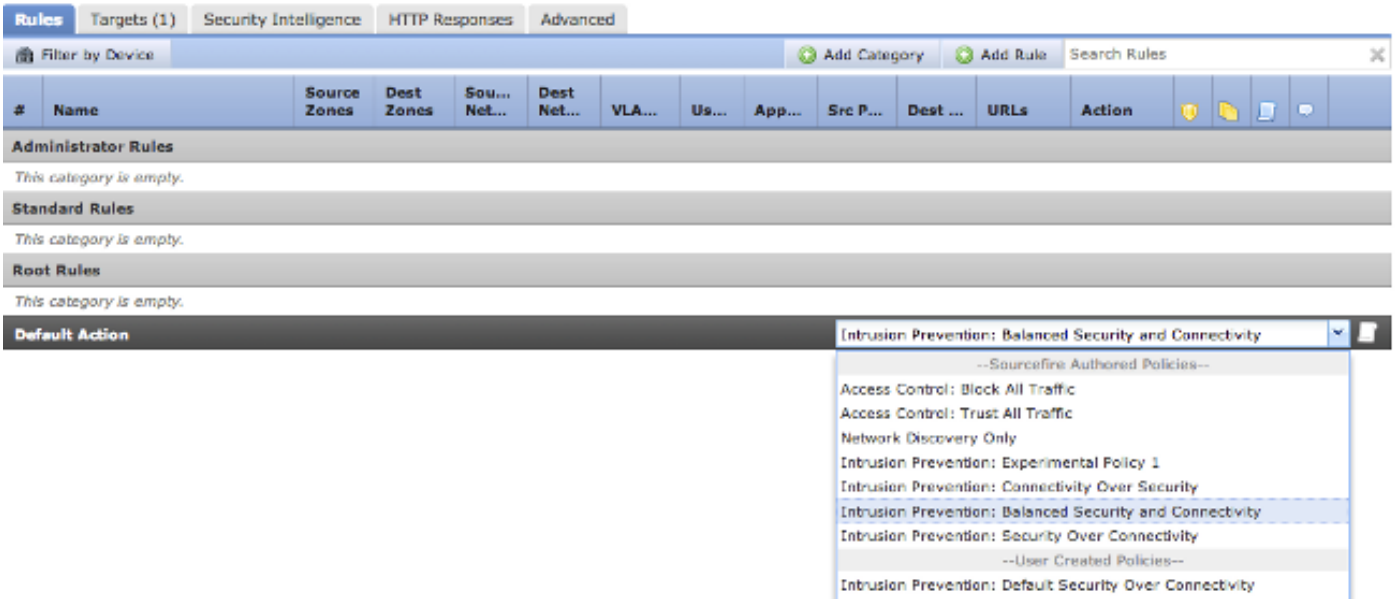


3. Geef een **naam** voor het beleid en een **beschrijving**.

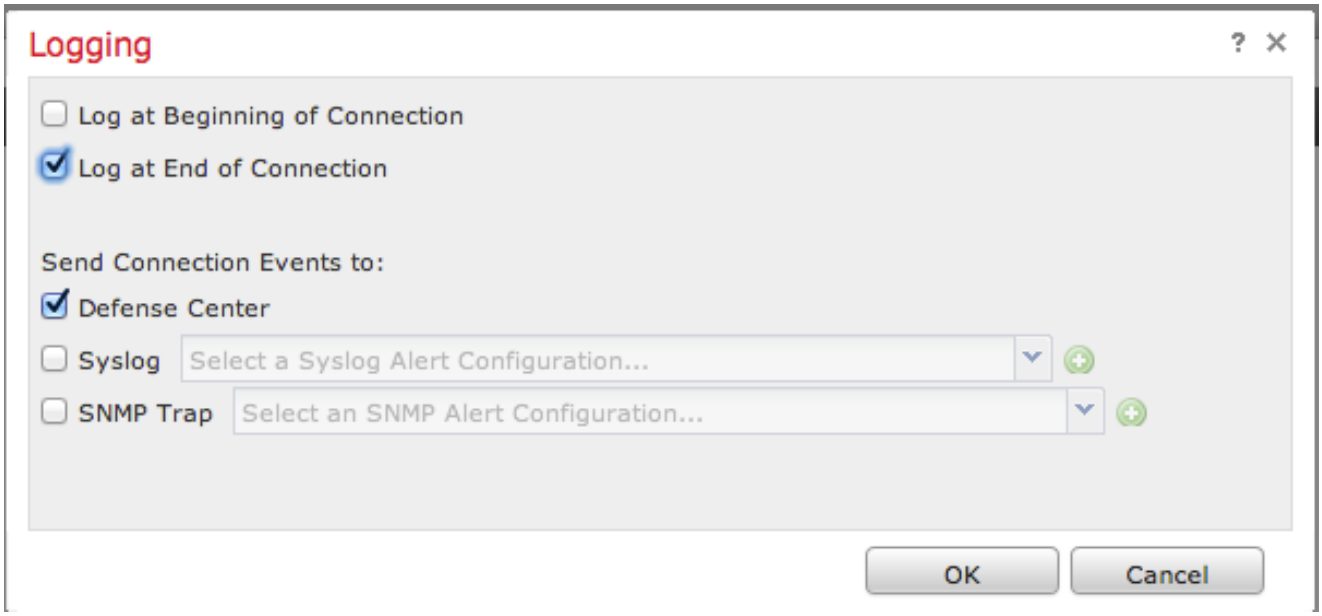
4. Selecteer **Inbraakpreventie** als de **standaardactie** van het toegangscontrolbeleid.

5. Selecteer ten slotte de **gerichte apparaten** waarop u het toegangscontrolemiddel wilt toepassen, en klik op **Opslaan**.

6. Selecteer uw inbraakbeleid voor de standaardactie.



7. De verbinding registreren moet worden ingeschakeld om verbindingsgebeurtenissen te genereren. Klik op het uitrolmenu dat rechts van de **Standaardactie** is.



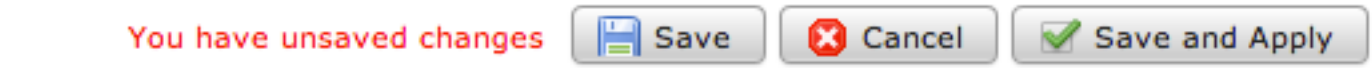
8. Klik erop om de verbindingen aan het begin of aan het eind van de verbinding te noteren. De gebeurtenissen kunnen worden vastgelegd op FireSIGHT Management Center, een actieve locatie of via SNMP.

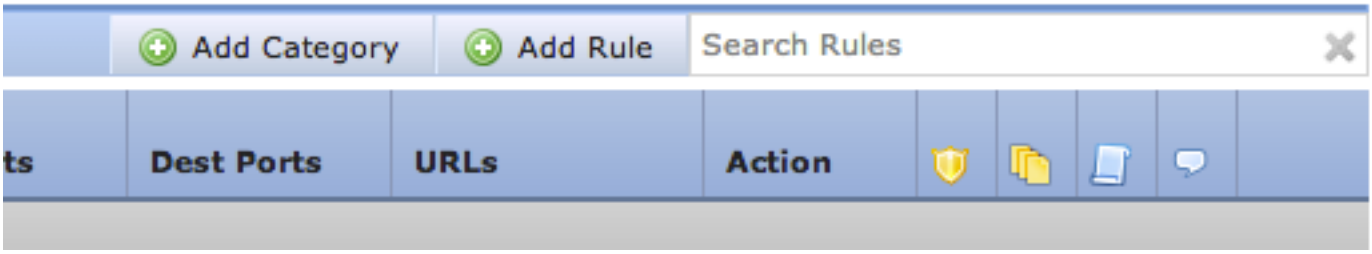
> Opmerking: Het is niet aanbevolen om aan beide uiteinden van de verbinding te loggen, omdat elke verbinding (behalve geblokkeerde verbindingen) twee keer zal worden vastgelegd. Loggen aan het begin is handig voor verbindingen die geblokkeerd zullen worden, en het registreren aan het eind is handig voor alle andere verbindingen.

9. Klik op **OK**. Merk op dat de kleur van het logingpictogram is gewijzigd.

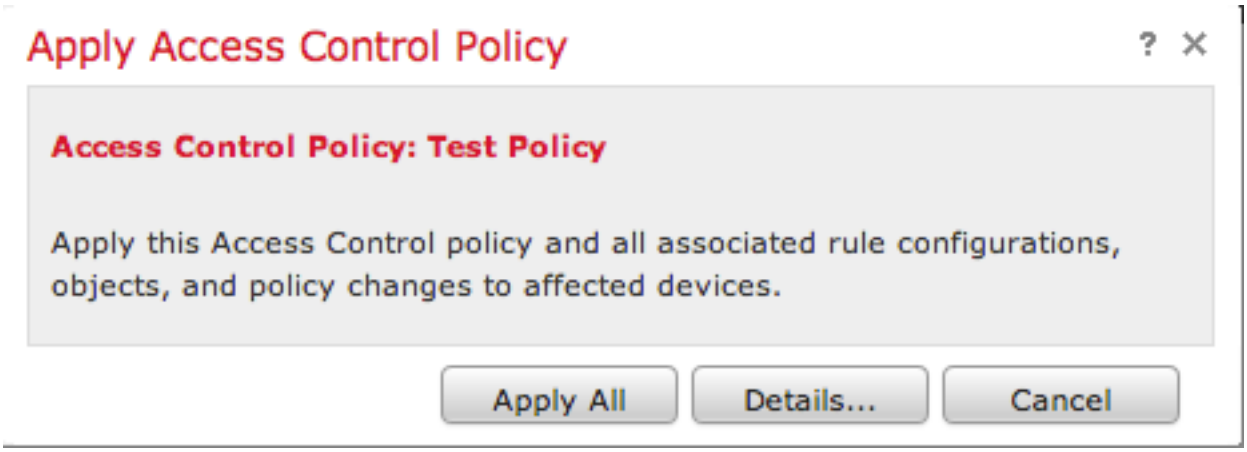
10. U kunt tegelijkertijd een **toegangscontroleregel** toevoegen. De opties die u kunt gebruiken zijn afhankelijk van het type licenties dat u hebt geïnstalleerd.

11. Als u klaar bent met het maken van wijzigingen. Klik op de knop **Opslaan en toepassen**. U merkt een bericht dat aangeeft dat u niet-opgeslagen wijzigingen in uw beleid in de rechterbovenhoek hebt uitgevoerd totdat op de knop is gedrukt.





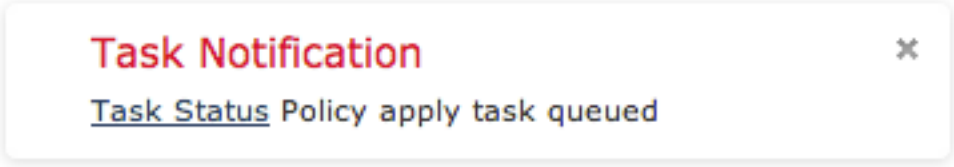
U kunt ervoor kiezen alleen de wijzigingen **op** te **slaan** of op **Opslaan en Toepassen** te klikken. Het volgende venster verschijnt als u het laatste kiest.



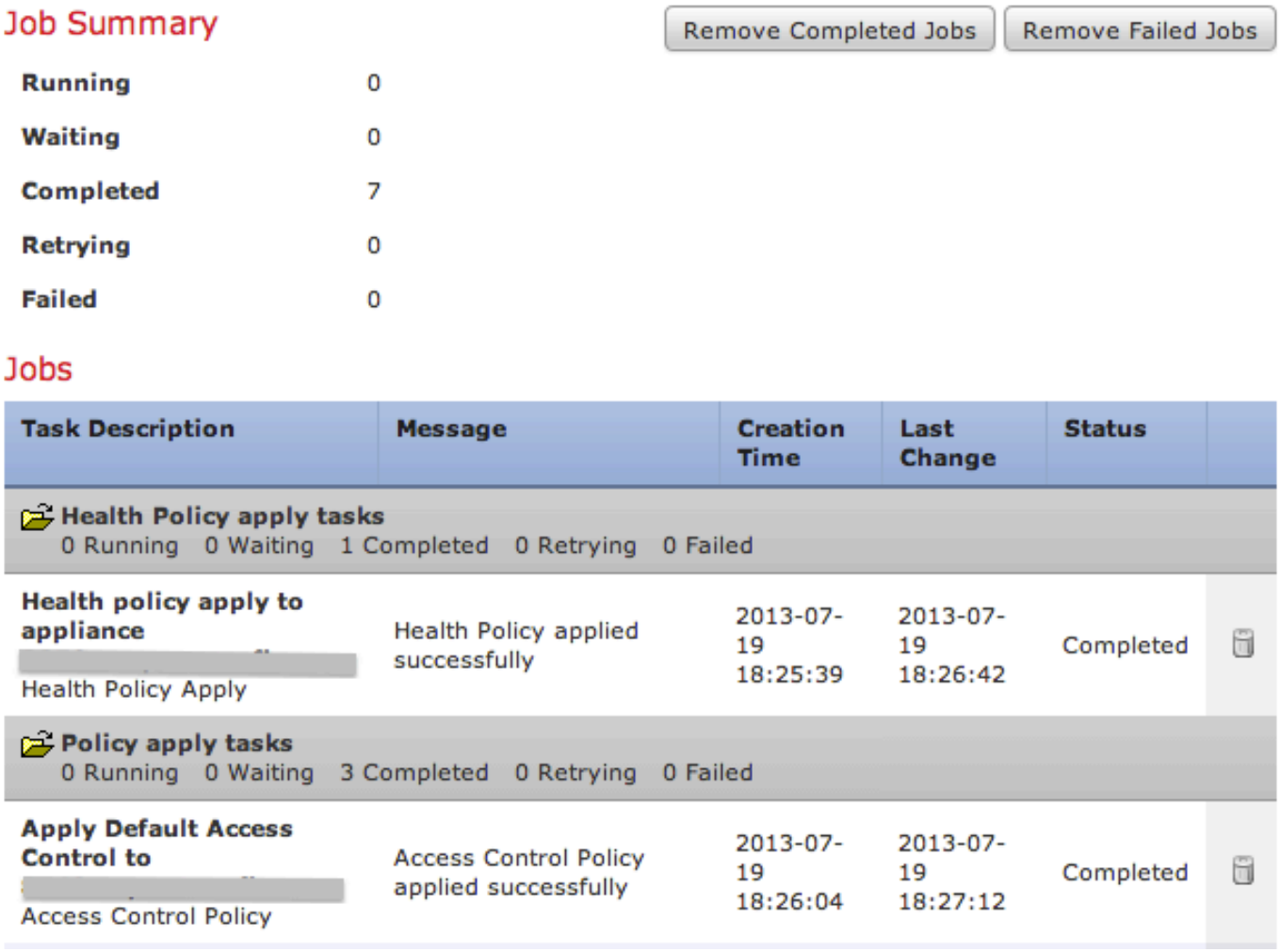
12. **Alles toepassen** zal het toegangscontrolebeleid en het (de) daaraan verbonden inbraakbeleid(en) op de beoogde voorzieningen toepassen.

> Opmerking: Als een inbraakbeleid voor het eerst wordt toegepast, kan het niet worden gedeselecteerd.

13. U kunt de status van de taak controleren door op de link **Taakstatus** te klikken in het bericht dat boven op de pagina wordt weergegeven, of door naar: **Systeem > Monitoring > Task Status**



14. Klik op de koppeling Taakstatus om de voortgang van het beleid voor toegangscontrole te controleren.



Stap 10: Controleer of het FireSIGHT Management Center gebeurtenissen heeft ontvangen

Nadat het beleid van de Toegangscontrole van toepassing is voltooid, zou u moeten beginnen om connecties gebeurtenissen te zien en afhankelijk van verkeer inbraakgebeurtenissen.

Aanvullende aanbeveling

U kunt ook de volgende aanvullende functies op uw systeem configureren. Raadpleeg de gebruikershandleiding voor meer informatie over de implementatie.

- Geplande back-ups
- Automatische softwareupdates, SRU, VDB en geoLocation downloads/installaties.
- Externe verificatie via LDAP of RADIUS