Fasi di configurazione iniziale dei sistemi FireSIGHT

Sommario

Introduzione

Dopo aver ricreato l'immagine di un centro di gestione FireSIGHT o di un dispositivo FirePOWER, è necessario completare diversi passaggi per rendere il sistema completamente funzionante e per generare avvisi per gli eventi di intrusione; ad esempio installazione della licenza, registrazione degli accessori, applicazione della policy di integrità, della policy di sistema, della policy di controllo dell'accesso, della policy antintrusione, ecc. Questo documento è un supplemento alla Guida all'installazione del sistema FireSIGHT.

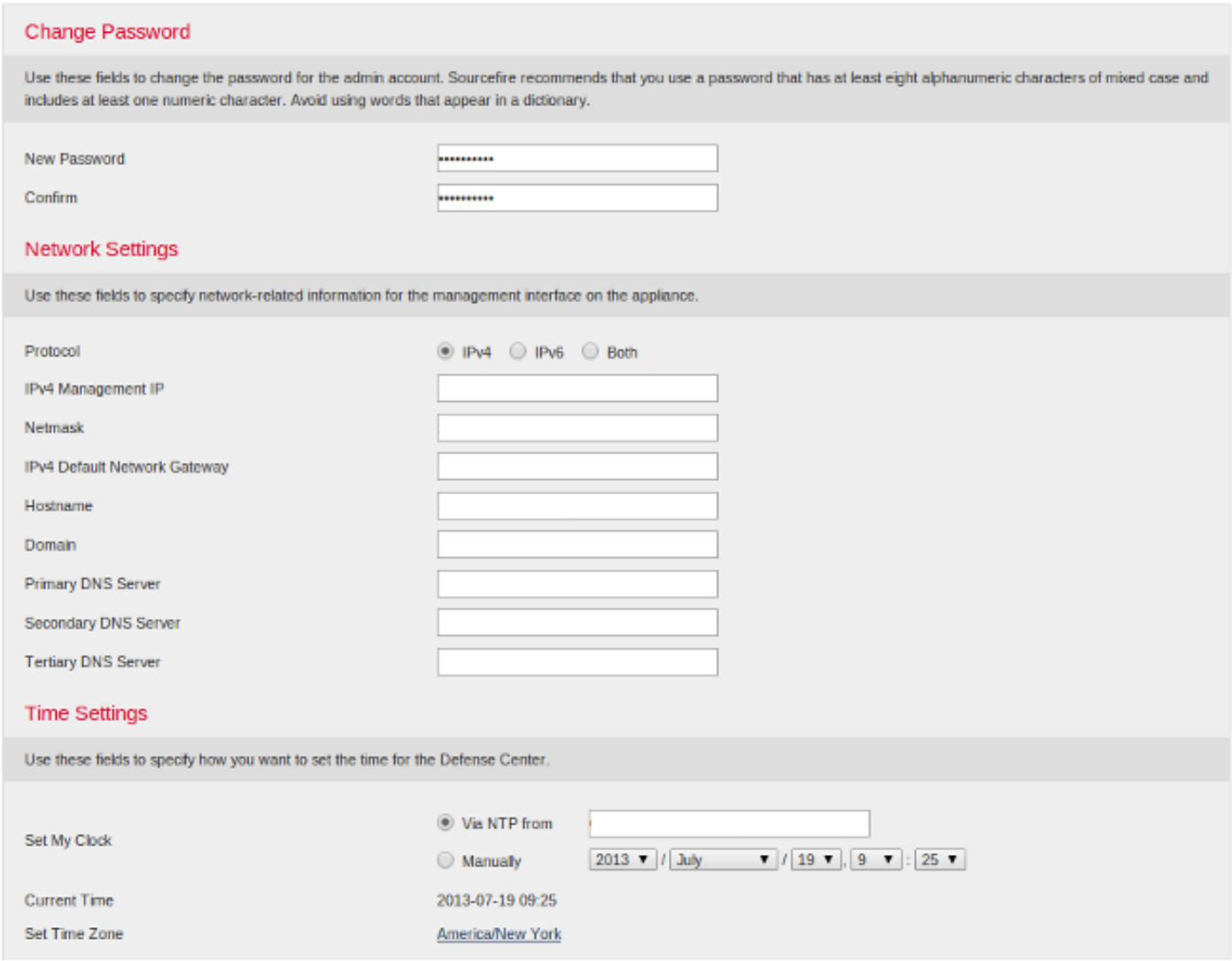
Prerequisito

Questa guida presuppone che l'utente abbia letto attentamente la Guida all'installazione del sistema FireSIGHT.

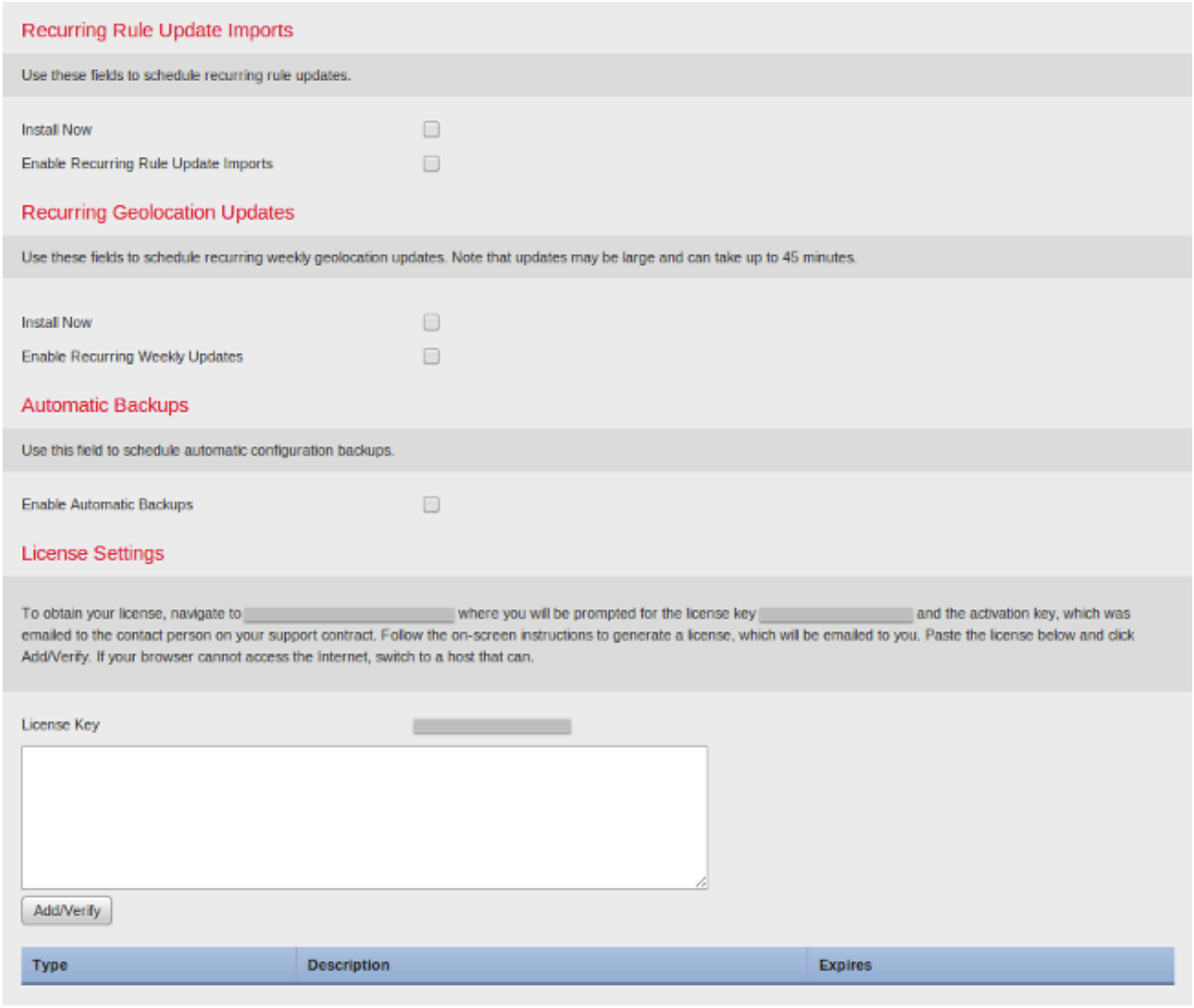
Configurazione

Passaggio 1: Configurazione iniziale

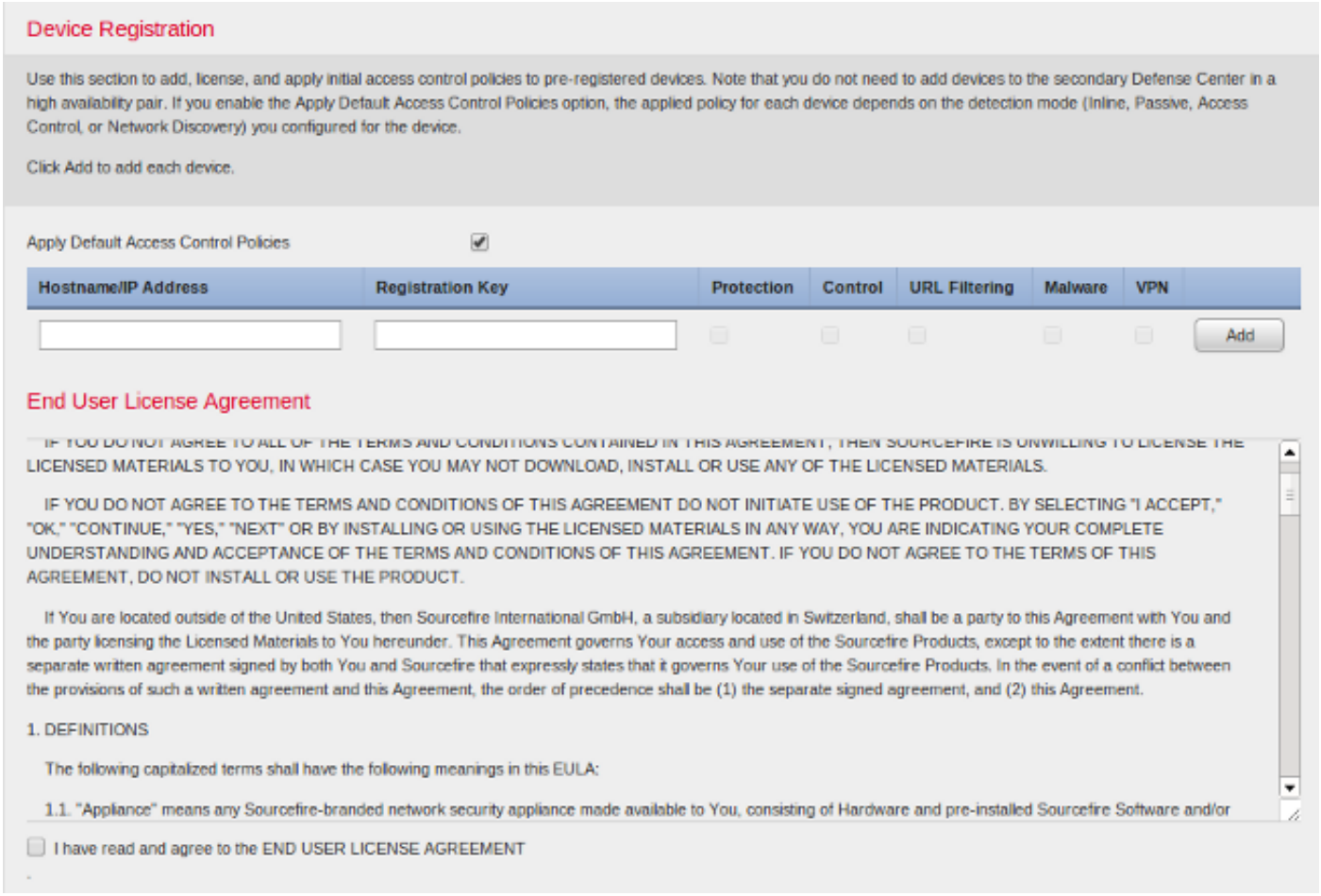
Sul centro di gestione FireSIGHT, è necessario completare il processo di configurazione accedendo all'interfaccia Web e specificando le opzioni di configurazione iniziale nella pagina di configurazione, illustrata di seguito. In questa pagina è necessario modificare la password dell'amministratore e specificare le impostazioni di rete, ad esempio i server DNS e di dominio, e la configurazione dell'ora.



Se lo si desidera, è possibile configurare aggiornamenti ricorrenti di regole e geolocalizzazione, nonché backup automatici. A questo punto è possibile installare anche le licenze per le funzionalità.



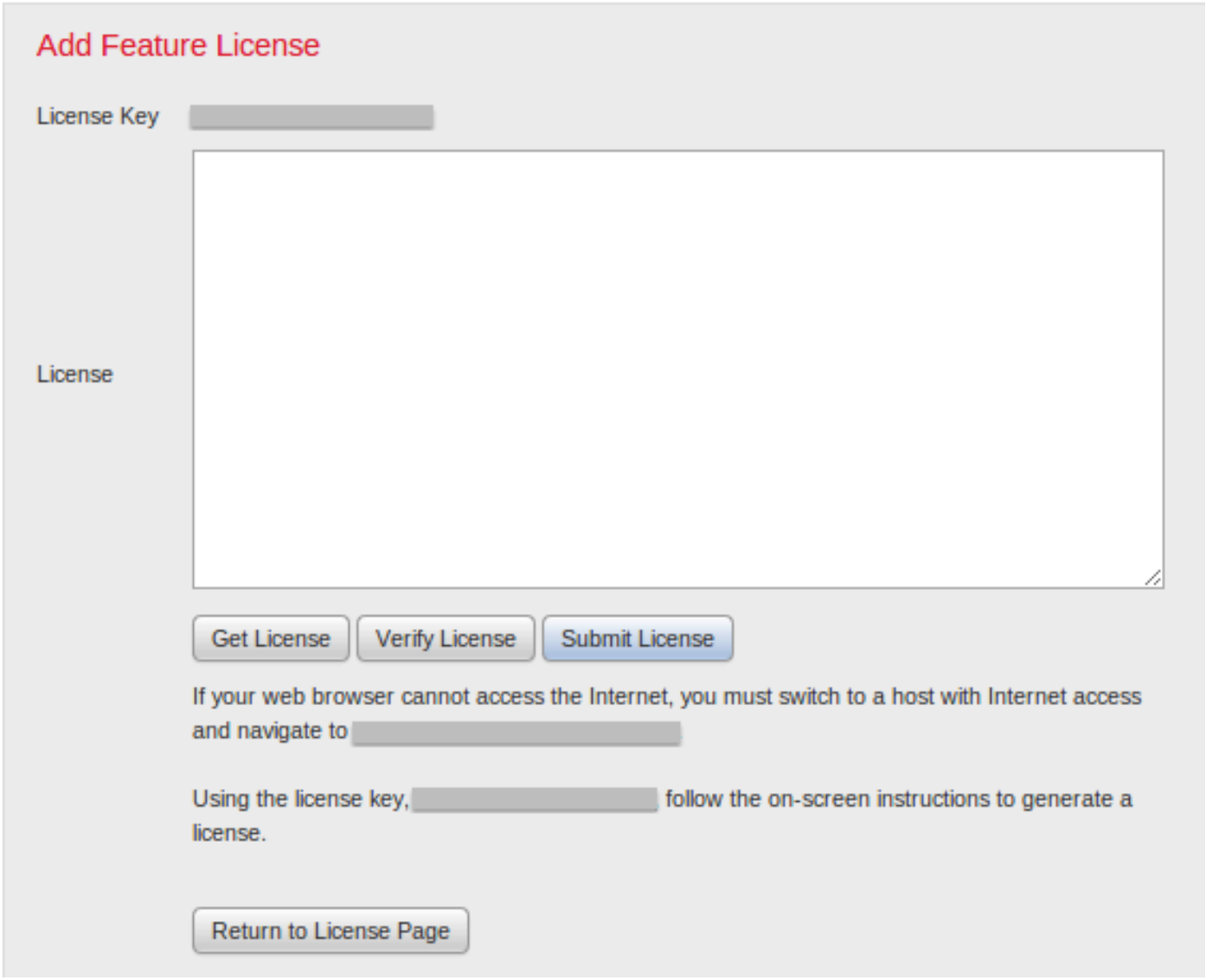
In questa pagina è inoltre possibile registrare un dispositivo nel centro di gestione FireSIGHT e specificare una modalità di rilevamento. La modalità di rilevamento e le altre opzioni scelte durante la registrazione determinano le interfacce predefinite, i set inline e le zone create dal sistema, nonché i criteri applicati inizialmente ai dispositivi gestiti.



Passaggio 2: Installa licenze

Se le licenze non sono state installate nella pagina di configurazione iniziale, è possibile completare l'operazione eseguendo la procedura seguente:

- Passare alla pagina seguente: **Sistema > Licenze**.
- Fare clic su **Add New License (Aggiungi nuova licenza)**.



Se non è stata ricevuta alcuna licenza, contattare il rappresentante commerciale dell'account.

Passaggio 3: Applica criteri di sistema

I criteri di sistema specificano la configurazione per i profili di autenticazione e la sincronizzazione dell'ora tra FireSIGHT Management Center e i dispositivi gestiti. Per configurare o applicare i criteri di sistema, selezionare **Sistema > Locale > Criteri di sistema**. È disponibile un criterio di sistema predefinito che deve essere applicato a qualsiasi dispositivo gestito.

Passaggio 4: Applica criteri di integrità

Il criterio di integrità viene utilizzato per configurare il modo in cui i dispositivi gestiti segnalano il proprio stato di integrità al centro di gestione FireSIGHT. Per configurare o applicare il criterio di integrità, passare a **Integrità > Criterio di integrità**. È disponibile un criterio di integrità predefinito che deve essere applicato a tutti i dispositivi gestiti.

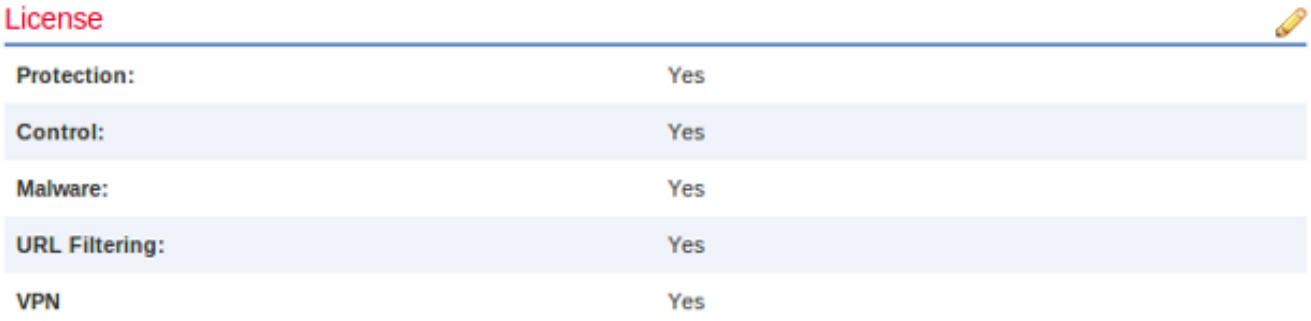
Passaggio 5: Registra dispositivi gestiti

Se non sono stati registrati dispositivi durante la pagina di configurazione iniziale, leggere questo documento per istruzioni su come registrare un dispositivo in un centro di gestione FireSIGHT.

Passaggio 6: Abilita licenze installate

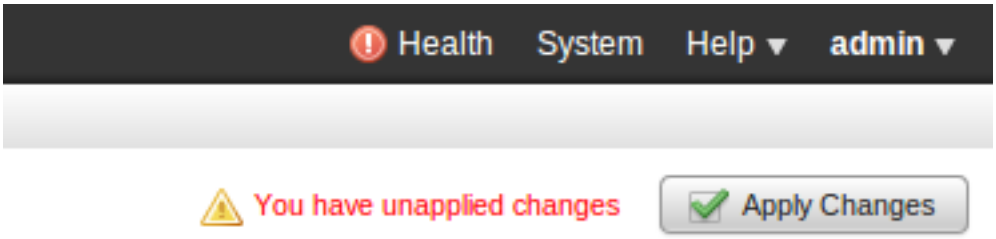
Prima di poter utilizzare qualsiasi licenza per le funzionalità sull'accessorio, è necessario attivarla per ciascun dispositivo gestito.

1. Passare alla pagina seguente: **Dispositivi > Gestione dispositivi**.
2. Fare clic sul dispositivo per il quale si desidera attivare le licenze e immettere la scheda Dispositivo.
3. Fare clic sull'icona **Edit** (*matita*) accanto a License (Licenza).



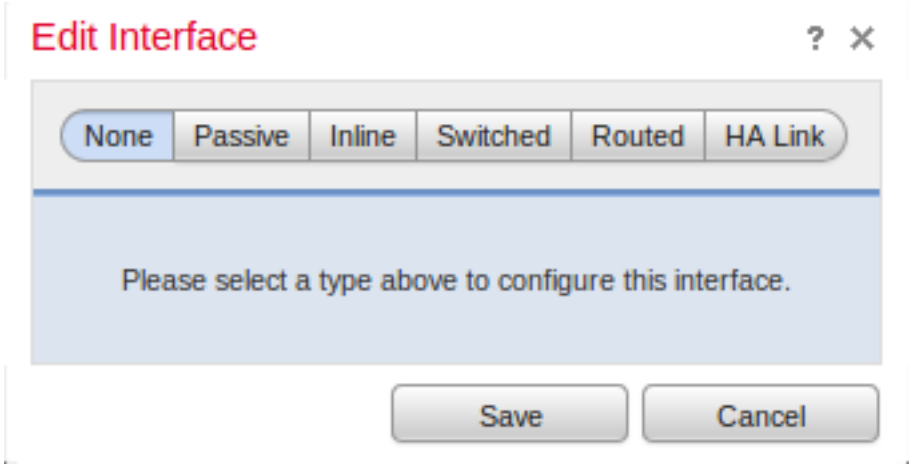
Abilitare le licenze richieste per il dispositivo e fare clic su **Salva**.

Notate il messaggio "*Avete apportato modifiche non applicate*" nell'angolo in alto a destra. Questo avviso rimane attivo anche se si esce dalla pagina di gestione dei dispositivi finché non si fa clic sul pulsante **Applica modifiche**.



Passaggio 7: Configurazione delle interfacce di rilevamento

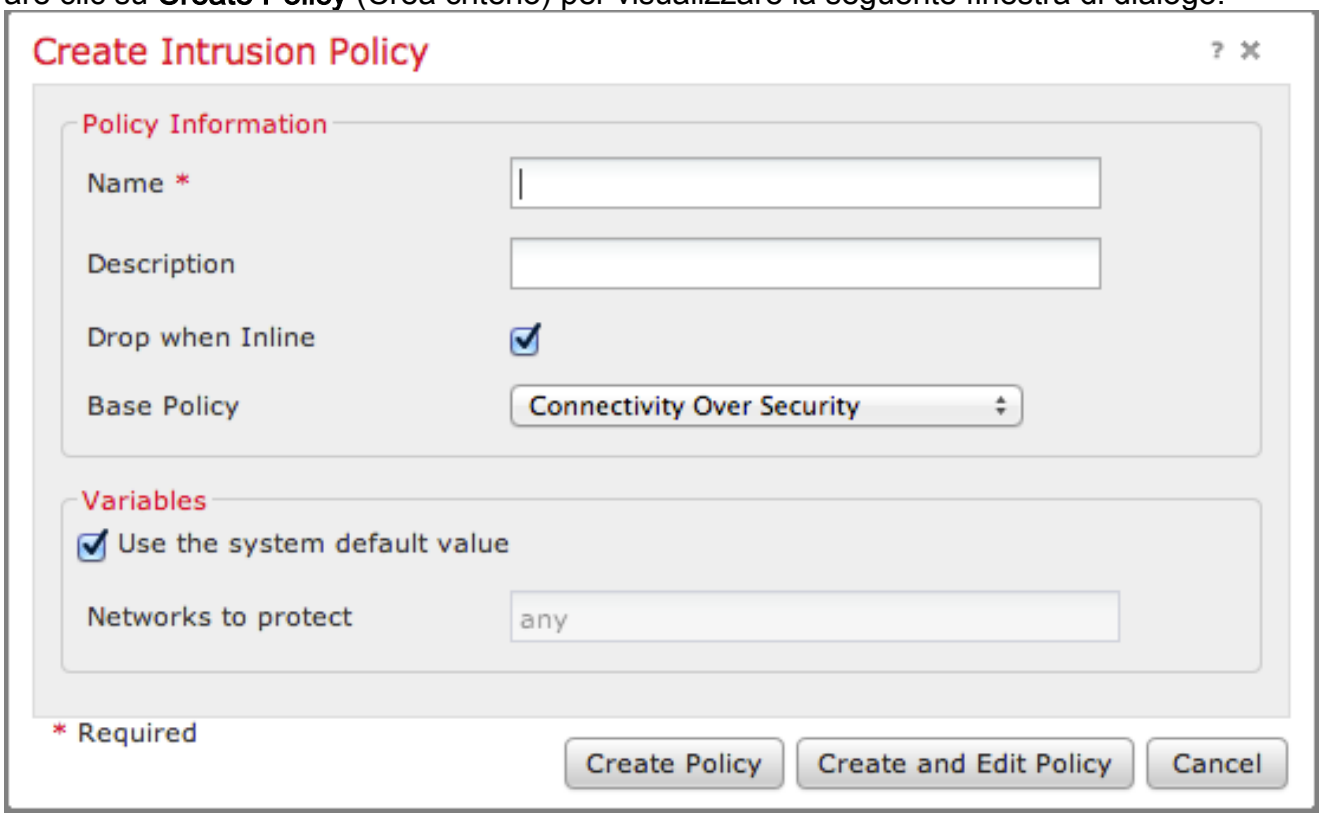
1. Passare alla pagina seguente **Dispositivi > Gestione dispositivi**.
2. Fare clic sull'icona **Modifica** (matita) per il sensore desiderato.
3. Nella scheda **Interfacce**, fare clic sull'icona **Modifica** per l'interfaccia desiderata.



Selezionare una configurazione di interfaccia passiva o inline. Le interfacce switched e routing esulano dall'ambito di questo articolo.

Passaggio 8: Configurare i criteri per le intrusioni

- Passare alla pagina seguente: **Policy > Intrusion > Intrusion Policy.**
- Fare clic su **Create Policy** (Crea criterio) per visualizzare la seguente finestra di dialogo:



Ènecessario assegnare un nome e definire il criterio di base da utilizzare. A seconda della distribuzione in uso, è possibile scegliere di attivare l'opzione **Elimina se in linea**. Definire le reti da proteggere per ridurre i falsi positivi e migliorare le prestazioni del sistema.

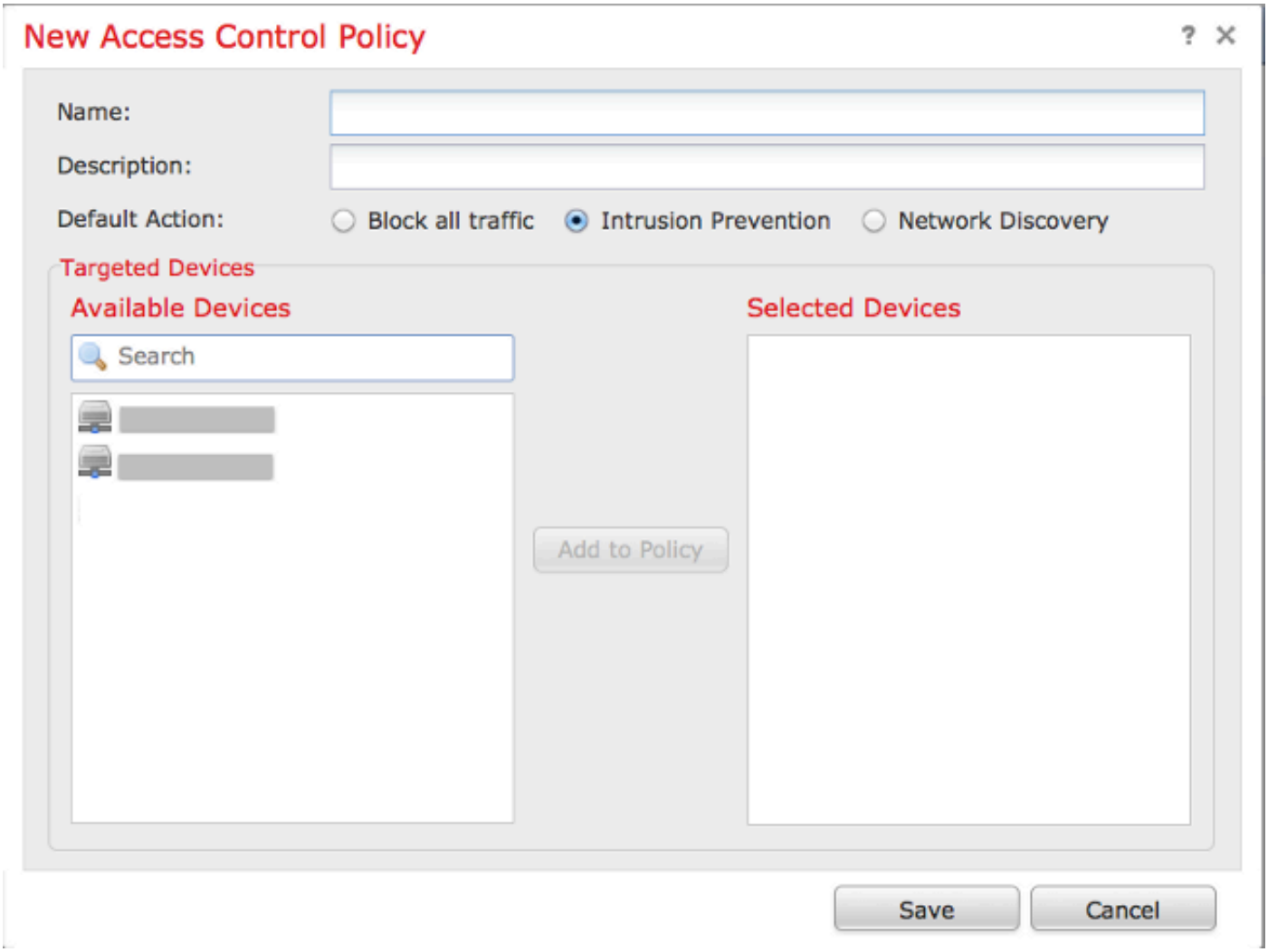
Se si fa clic su **Crea criterio**, le impostazioni verranno salvate e verrà creato il criterio IPS. Se si desidera apportare modifiche al criterio per le intrusioni, è invece possibile scegliere **Crea e modifica criterio**.

Nota: I criteri per le intrusioni vengono applicati come parte dei criteri di controllo di accesso. Dopo aver applicato un criterio Intrusion, è possibile applicare le modifiche senza riapplicare l'intero criterio di controllo dell'accesso facendo clic sul pulsante **Riapplica**.

Passaggio 9: Configurare e applicare un criterio di controllo dell'accesso

1. Passare a **Criteri > Controllo accesso**.

2. Fare clic su **Nuovo criterio**.

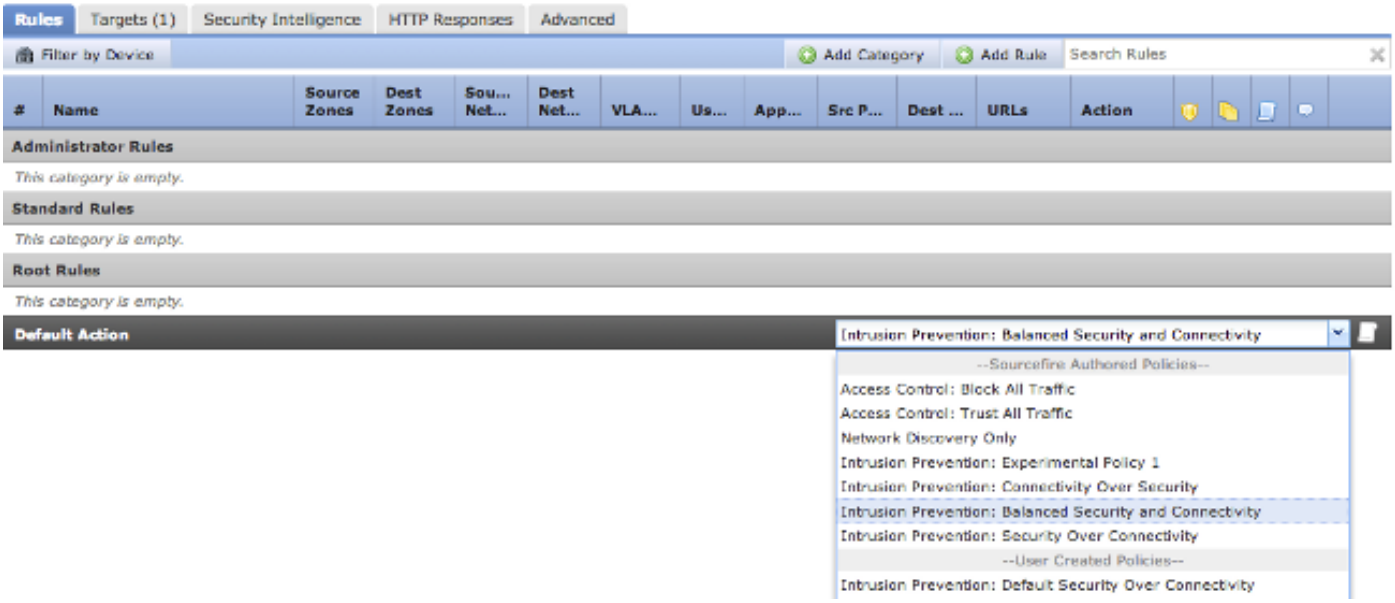


3. Specificare un **nome** per il criterio e una **descrizione**.

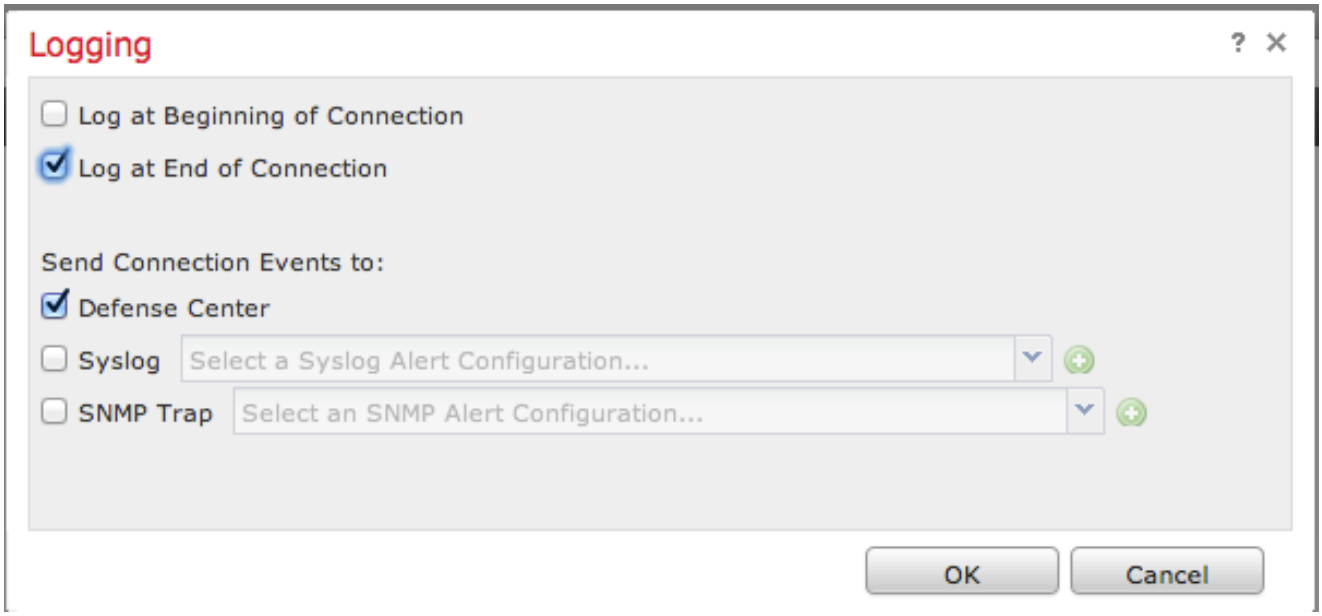
4. Selezionare **Prevenzione intrusioni** come **azione predefinita** dei criteri di controllo di accesso.

5. Selezionare infine le **Periferiche di destinazione** a cui si desidera applicare la policy di controllo dell'accesso e fare clic su **Salva**.

6. Selezionare il criterio di intrusione per l'azione predefinita.



7. Per generare eventi di connessione, è necessario abilitare la registrazione delle connessioni. Fare clic sul menu a discesa a destra di **Azione predefinita**.



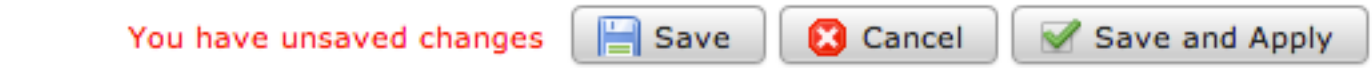
8. Scegliere di registrare le connessioni all'inizio o alla fine della connessione. Gli eventi possono essere registrati su FireSIGHT Management Center, una posizione syslog o tramite SNMP.

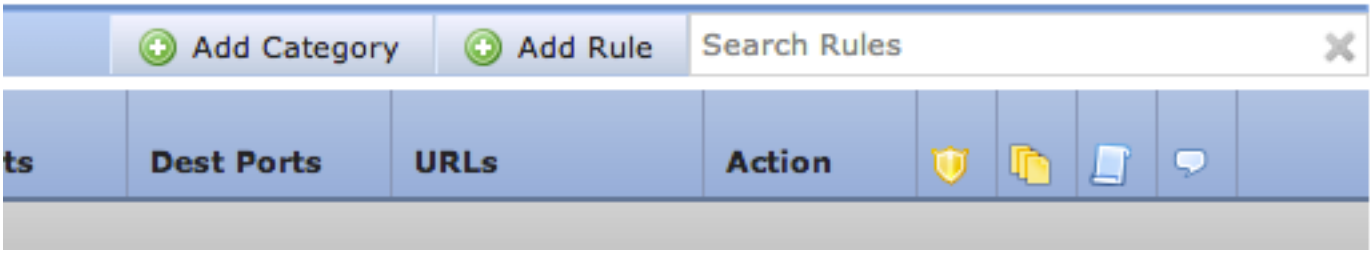
> **Nota:** Non è consigliabile eseguire l'accesso a entrambe le estremità della connessione perché ogni connessione, ad eccezione di quelle bloccate, verrà registrata due volte. La registrazione all'inizio è utile per le connessioni che verranno bloccate, mentre la registrazione alla fine è utile per tutte le altre connessioni.

9. Fare clic su **OK**. Il colore dell'icona di registrazione è cambiato.

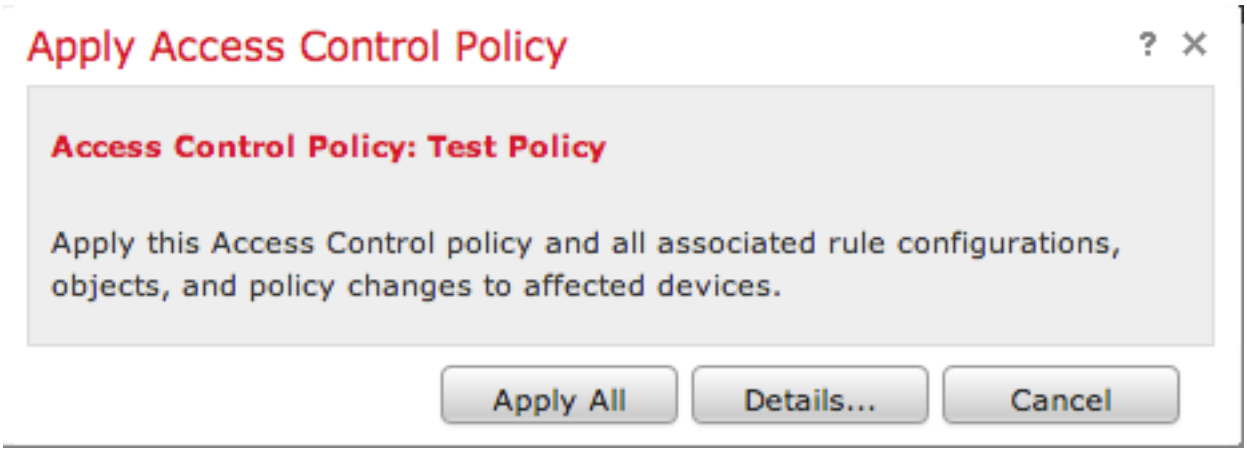
10. È possibile aggiungere una **regola di controllo di accesso** in questo momento. Le opzioni disponibili dipendono dal tipo di licenze installate.

11. Dopo aver apportato le modifiche desiderate. fare clic sul pulsante **Salva e applica**. Verrà visualizzato un messaggio che indica che sono presenti modifiche non salvate nel criterio nell'angolo superiore destro finché non si fa clic sul pulsante.





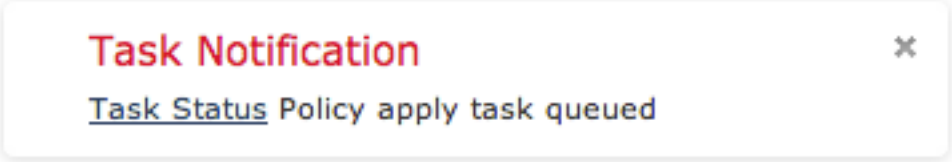
È possibile scegliere di **salvare** solo le modifiche o fare clic su **Salva e applica**. Se si sceglie quest'ultima, viene visualizzata la seguente finestra.



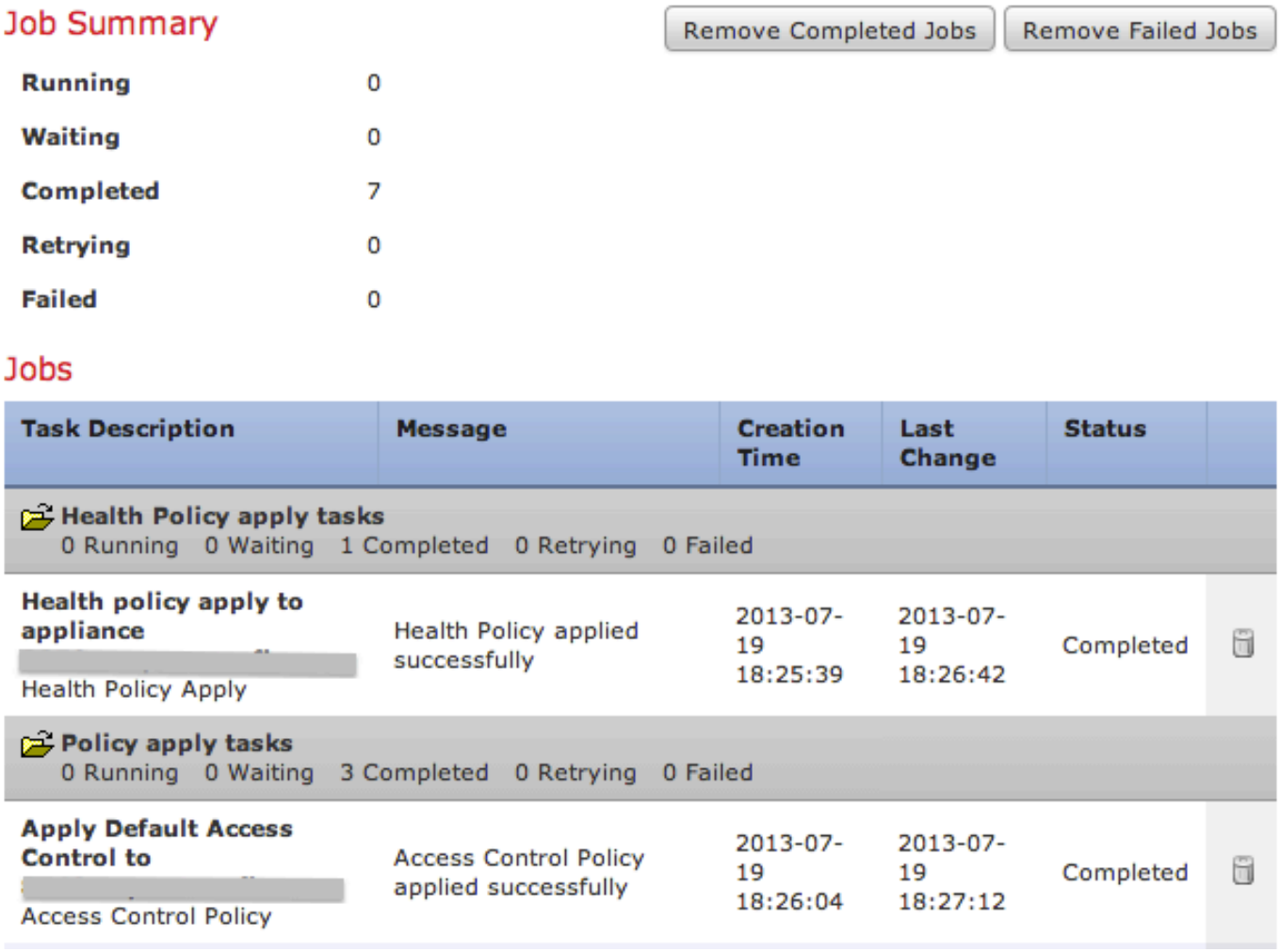
12. **Apply All (Applica tutto)** applicherà la policy di controllo dell'accesso e le policy sulle intrusioni associate ai dispositivi di destinazione.

> **Nota:** Se un criterio di intrusione verrà applicato per la prima volta, non sarà possibile deselezionarlo.

13. È possibile controllare lo stato del task facendo clic sul collegamento **Stato task** nella notifica visualizzata nella parte superiore della pagina oppure passando a: **Sistema > Monitoraggio > Stato task**



14. Fare clic sul collegamento Stato task per controllare lo stato di avanzamento dell'applicazione dei criteri di controllo di accesso.



Passaggio 10: Verifica della ricezione di eventi da parte di FireSIGHT Management Center

Al termine dell'applicazione dei criteri di controllo di accesso, è consigliabile iniziare a visualizzare gli eventi di connessione e a seconda degli eventi di intrusione nel traffico.

Ulteriori suggerimenti

Èinoltre possibile configurare le seguenti funzionalità aggiuntive nel sistema. Per ulteriori informazioni sull'implementazione, consultare la Guida dell'utente.

- Backup pianificati
- Aggiornamenti automatici del software, SRU, VDB e download/installazioni GeoLocation.
- Autenticazione esterna tramite LDAP o RADIUS