

# Fasi di configurazione iniziale dei sistemi FireSIGHT

## Sommario

[Introduzione](#)

[Prerequisito](#)

[Configurazione](#)

[Passaggio 1: Configurazione iniziale](#)

[Passaggio 2: Installa licenze](#)

[Passaggio 3: Applica criteri di sistema](#)

[Passaggio 4: Applica criteri di integrità](#)

[Passaggio 5: Registra dispositivi gestiti](#)

[Passaggio 6: Abilita licenze installate](#)

[Passaggio 7: Configurazione delle interfacce di rilevamento](#)

[Passaggio 8: Configurare i criteri per le intrusioni](#)

[Passaggio 9: Configurare e applicare un criterio di controllo dell'accesso](#)

[Passaggio 10: Verifica della ricezione di eventi da parte di FireSIGHT Management Center](#)

[Ulteriori suggerimenti](#)

## 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.

**Change Password**

Use these fields to change the password for the admin account. Sourcefire recommends that you use a password that has at least eight alphanumeric characters of mixed case and includes at least one numeric character. Avoid using words that appear in a dictionary.

New Password

Confirm

**Network Settings**

Use these fields to specify network-related information for the management interface on the appliance.

Protocol  IPv4  IPv6  Both

IPv4 Management IP

Netmask

IPv4 Default Network Gateway

Hostname

Domain

Primary DNS Server

Secondary DNS Server

Tertiary DNS Server

**Time Settings**

Use these fields to specify how you want to set the time for the Defense Center.

Set My Clock  Via NTP from

Manually 2013 ▾ / July ▾ / 19 ▾ , 9 ▾ : 25 ▾

Current Time 2013-07-19 09:25

Set Time Zone [America/New York](#)

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.

### Recurring Rule Update Imports

Use these fields to schedule recurring rule updates.

Install Now

Enable Recurring Rule Update Imports

### Recurring Geolocation Updates

Use these fields to schedule recurring weekly geolocation updates. Note that updates may be large and can take up to 45 minutes.

Install Now

Enable Recurring Weekly Updates

### Automatic Backups

Use this field to schedule automatic configuration backups.

Enable Automatic Backups

### License Settings

To obtain your license, navigate to \_\_\_\_\_ where you will be prompted for the license key \_\_\_\_\_ and the activation key, which was emailed to the contact person on your support contract. Follow the on-screen instructions to generate a license, which will be emailed to you. Paste the license below and click Add/Verify. If your browser cannot access the Internet, switch to a host that can.

License Key \_\_\_\_\_

Add/Verify

Type	Description	Expires
------	-------------	---------

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.

## Device Registration

Use this section to add, license, and apply initial access control policies to pre-registered devices. Note that you do not need to add devices to the secondary Defense Center in a high availability pair. If you enable the Apply Default Access Control Policies option, the applied policy for each device depends on the detection mode (Inline, Passive, Access Control, or Network Discovery) you configured for the device.

Click Add to add each device.

Apply Default Access Control Policies

Hostname/IP Address	Registration Key	Protection	Control	URL Filtering	Malware	VPN	
<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="button" value="Add"/>

## End User License Agreement

IF YOU DO NOT AGREE TO ALL OF THE TERMS AND CONDITIONS CONTAINED IN THIS AGREEMENT, THEN SOURCEFIRE IS UNWILLING TO LICENSE THE LICENSED MATERIALS TO YOU, IN WHICH CASE YOU MAY NOT DOWNLOAD, INSTALL OR USE ANY OF THE LICENSED MATERIALS.

IF YOU DO NOT AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT DO NOT INITIATE USE OF THE PRODUCT. BY SELECTING "I ACCEPT," "OK," "CONTINUE," "YES," "NEXT" OR BY INSTALLING OR USING THE LICENSED MATERIALS IN ANY WAY, YOU ARE INDICATING YOUR COMPLETE UNDERSTANDING AND ACCEPTANCE OF THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, DO NOT INSTALL OR USE THE PRODUCT.

If You are located outside of the United States, then Sourcefire International GmbH, a subsidiary located in Switzerland, shall be a party to this Agreement with You and the party licensing the Licensed Materials to You hereunder. This Agreement governs Your access and use of the Sourcefire Products, except to the extent there is a separate written agreement signed by both You and Sourcefire that expressly states that it governs Your use of the Sourcefire Products. In the event of a conflict between the provisions of such a written agreement and this Agreement, the order of precedence shall be (1) the separate signed agreement, and (2) this Agreement.

### 1. DEFINITIONS

The following capitalized terms shall have the following meanings in this EULA:

1.1. "Appliance" means any Sourcefire-branded network security appliance made available to You, consisting of Hardware and pre-installed Sourcefire Software and/or

I have read and agree to the END USER LICENSE AGREEMENT

## 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)**.

## Add Feature License

License Key

License

If your web browser cannot access the Internet, you must switch to a host with Internet access and navigate to

Using the license key,  follow the on-screen instructions to generate a license.

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.

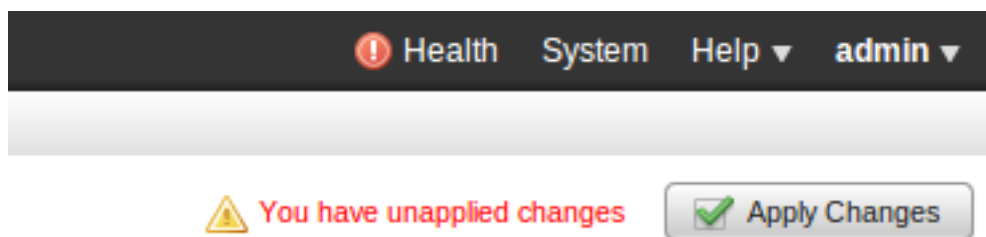
1. Passare alla pagina seguente: **Dispositivi > Gestione dispositivi**.
2. Fare clic sul dispositivo per il quale si desidera attivare le licenze e immettere la scheda Dispositivo.
3. Fare clic sull'icona **Edit** (*matita*) accanto a License (Licenza).

### License

Protection:	Yes
Control:	Yes
Malware:	Yes
URL Filtering:	Yes
VPN	Yes

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.

**Edit Interface** ? X

None Passive Inline Switched Routed HA Link

Please select a type above to configure this interface.

Save Cancel

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:

**Create Intrusion Policy** ? X

**Policy Information**

Name \*

Description

Drop when Inline

Base Policy

**Variables**

Use the system default value

Networks to protect

\* Required

Create Policy Create and Edit Policy Cancel

È necessario 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**.

**New Access Control Policy** ? X

Name:

Description:

Default Action:  Block all traffic  Intrusion Prevention  Network Discovery

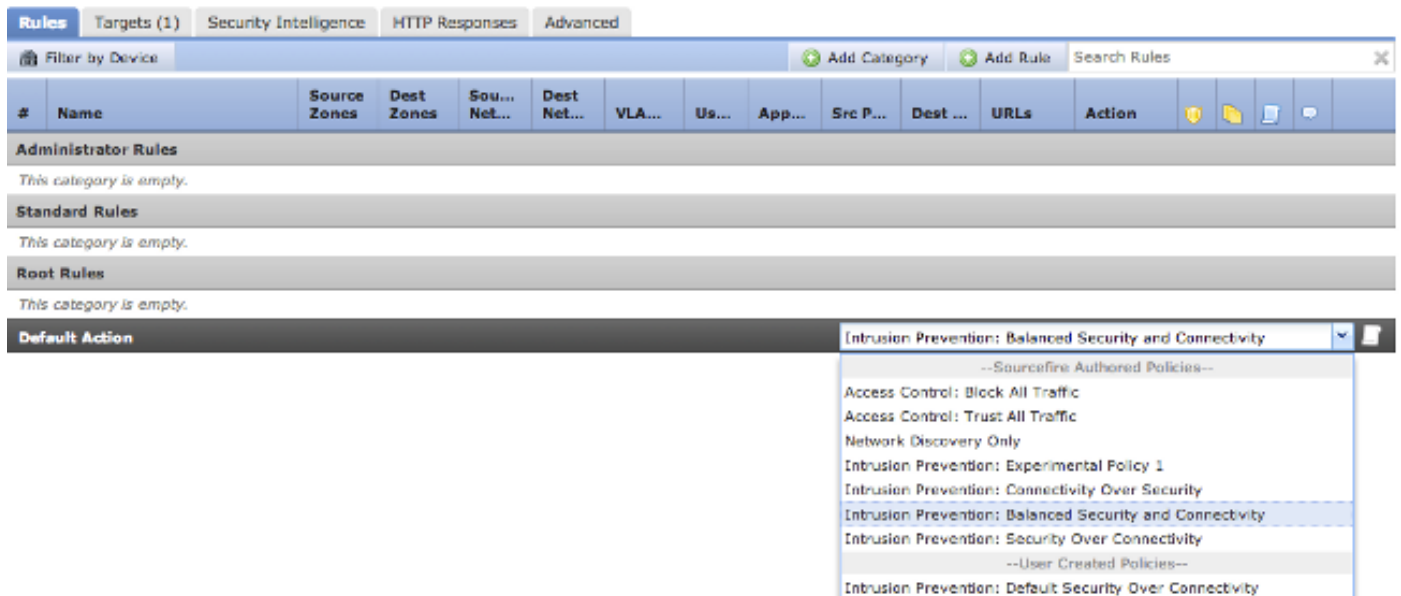
**Targeted Devices**

**Available Devices**

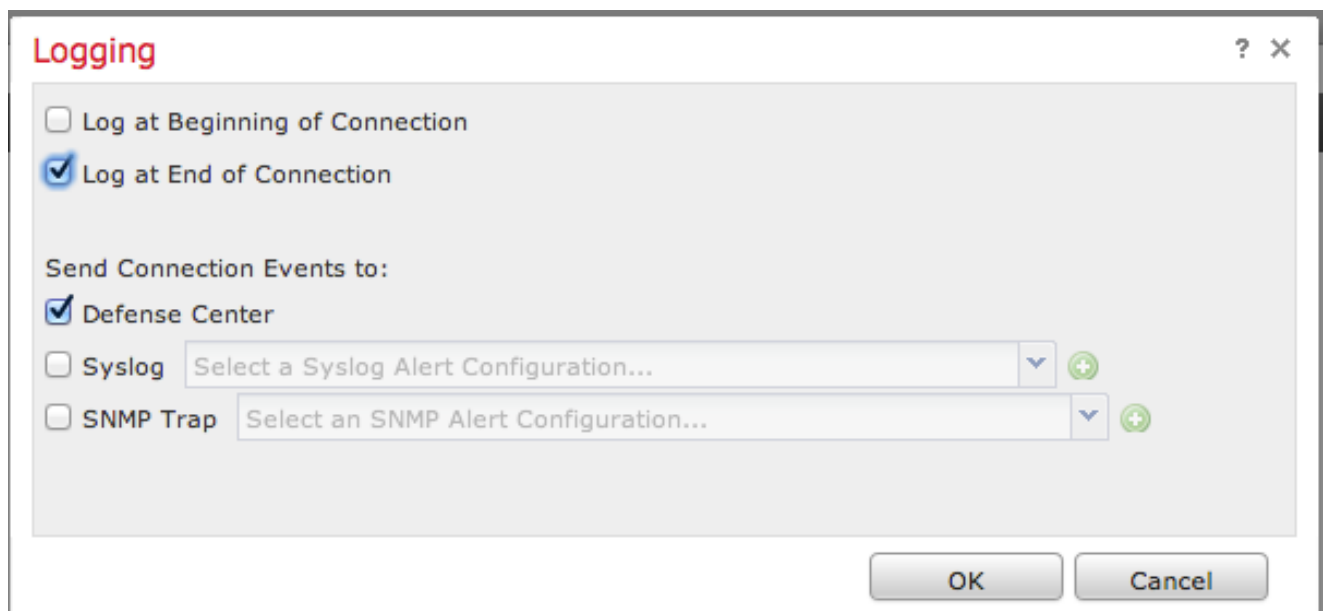
**Selected Devices**

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.

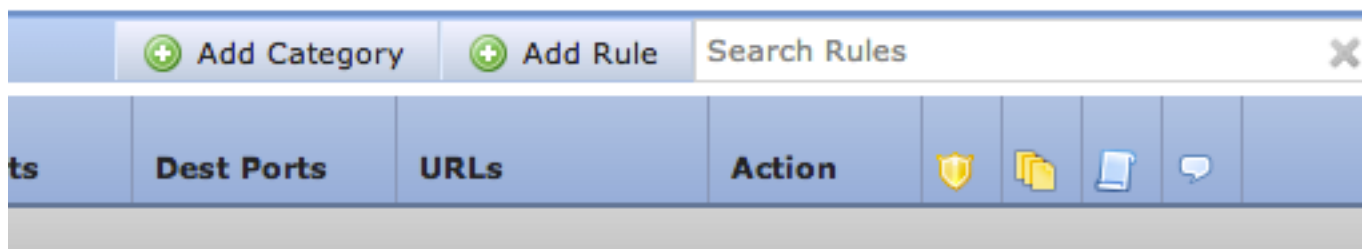
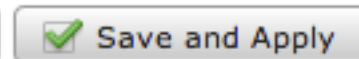
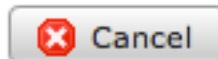
**Nota:** Non è consigliabile eseguire l'accesso a entrambe le estremità della connessione perché ogni connessione, ad eccezione di quelle bloccate, verrà registrata due volte. La registrazione all'inizio è utile per le connessioni che verranno bloccate, mentre la registrazione alla fine è utile per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

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

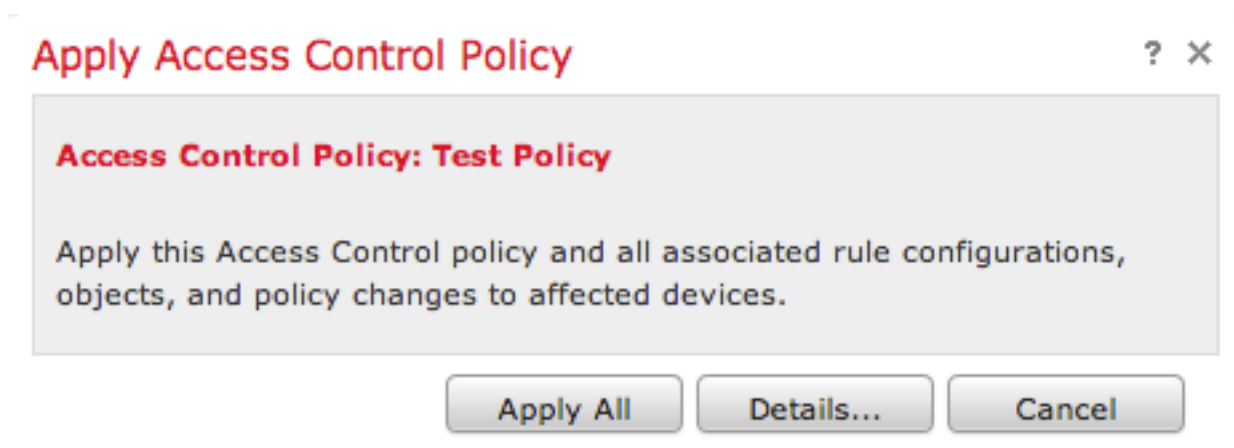
10. È possibile aggiungere una **regola di controllo di accesso** in questo momento. Le opzioni disponibili dipendono dal tipo di licenze installate.

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.

You have unsaved changes



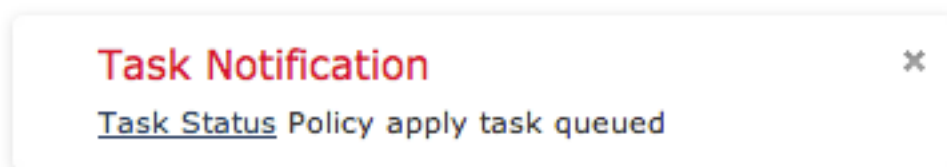
È possibile scegliere di **salvare** solo le modifiche o fare clic su **Salva e applica**. Se si sceglie quest'ultima, viene visualizzata la seguente finestra.



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 deseleggerlo.

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.





## Job Summary

Remove Completed Jobs

Remove Failed Jobs

Running	0
Waiting	0
Completed	7
Retrying	0
Failed	0

## Jobs

Task Description	Message	Creation Time	Last Change	Status	
 <b>Health Policy apply tasks</b> 0 Running 0 Waiting 1 Completed 0 Retrying 0 Failed					
<b>Health policy apply to appliance</b> [redacted] Health Policy Apply	Health Policy applied successfully	2013-07-19 18:25:39	2013-07-19 18:26:42	Completed	
 <b>Policy apply tasks</b> 0 Running 0 Waiting 3 Completed 0 Retrying 0 Failed					
<b>Apply Default Access Control to</b> [redacted] Access Control Policy	Access Control Policy applied successfully	2013-07-19 18:26:04	2013-07-19 18:27:12	Completed	

## 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

È inoltre 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