

# Anfängliche Konfigurationsschritte bei FireSIGHT-Systemen

## Inhalt

[Einführung](#)

[Voraussetzung](#)

[Konfiguration](#)

[Schritt 1: Ersteinrichtung](#)

[Schritt 2: Installieren von Lizenzen](#)

[Schritt 3: Anwenden der Systemrichtlinie](#)

[Schritt 4: Anwendung der Gesundheitspolitik](#)

[Schritt 5: Registrieren verwalteter Geräte](#)

[Schritt 6: Aktivieren installierter Lizenzen](#)

[Schritt 7: Konfigurieren von Sensorschnittstellen](#)

[Schritt 8: Konfigurieren der Intrusion Policy](#)

[Schritt 9: Konfiguration und Anwendung einer Zugriffskontrollrichtlinie](#)

[Schritt 10: Überprüfen, ob das FireSIGHT Management Center Ereignisse empfängt](#)

[Zusätzliche Empfehlung](#)

## Einführung

Nachdem Sie ein neues Image eines FireSIGHT Management Center oder eines FirePOWER-Geräts erstellt haben, müssen Sie mehrere Schritte ausführen, um das System voll funktionsfähig zu machen und Warnmeldungen für Angriffsversuche zu generieren. z. B. Installation von Lizenzen, Registrierung von Appliances, Anwendung von Integritätsrichtlinien, Systemrichtlinien, Zugriffskontrollrichtlinien, Zugriffsrichtlinien usw. Dieses Dokument ist eine Ergänzung zum FireSIGHT System Installation Guide.

## Voraussetzung

In diesem Handbuch wird davon ausgegangen, dass Sie die FireSIGHT-Systeminstallationsanleitung sorgfältig gelesen haben.

## Konfiguration

### Schritt 1: Ersteinrichtung

Sie müssen den Setup-Prozess auf Ihrem FireSIGHT Management Center abschließen, indem Sie sich bei der Webschnittstelle anmelden und auf der unten abgebildeten Einrichtungsseite Optionen für die Erstkonfiguration festlegen. Auf dieser Seite müssen Sie das Administratorkennwort ändern und können außerdem Netzwerkeinstellungen wie Domänen- und DNS-Server und die Zeitkonfiguration angeben.

**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  /  /  ,  :

Current Time 2013-07-19 09:25

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

Sie können optional wiederkehrende Regel- und Standortaktualisierungen sowie automatische Sicherungen konfigurieren. Zu diesem Zeitpunkt können auch alle Funktionslizenzen installiert werden.

### 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
------	-------------	---------

Auf dieser Seite können Sie auch ein Gerät im FireSIGHT Management Center registrieren und einen Erkennungsmodus angeben. Der Erkennungsmodus und andere Optionen, die Sie bei der Registrierung auswählen, bestimmen die vom System erstellten Standardschnittstellen, Inlinesätze und Zonen sowie die Richtlinien, die es ursprünglich auf verwaltete Geräte anwendet.

## 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="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

## Schritt 2: Installieren von Lizenzen

Wenn Sie die Lizenzen während der Ersteinrichtung nicht installiert haben, gehen Sie wie folgt vor:

- Navigieren Sie zur folgenden Seite: **System > Lizenzen**.
- Klicken Sie auf **Neue Lizenz hinzufügen**.

## 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.

Wenn Sie keine Lizenz erhalten haben, wenden Sie sich an den Vertriebsmitarbeiter Ihres Kontos.

### Schritt 3: Anwenden der Systemrichtlinie

Die Systemrichtlinie legt die Konfiguration für Authentifizierungsprofile und Zeitsynchronisierung zwischen dem FireSIGHT Management Center und verwalteten Geräten fest. Um die Systemrichtlinie zu konfigurieren oder anzuwenden, navigieren Sie zu **System > Local > System Policy (System > Lokal > Systemrichtlinie)**. Es wird eine Standard-Systemrichtlinie bereitgestellt, die jedoch auf alle verwalteten Geräte angewendet werden muss.

### Schritt 4: Anwendung der Gesundheitspolitik

Die Health Policy wird verwendet, um zu konfigurieren, wie verwaltete Geräte ihren Gesundheitsstatus an das FireSIGHT Management Center melden. Um die Gesundheitsrichtlinie zu konfigurieren oder anzuwenden, navigieren Sie zu **Health > Health Policy**. Es wird eine Standard-Integritätsrichtlinie bereitgestellt, die jedoch auf alle verwalteten Geräte angewendet werden muss.

## Schritt 5: Registrieren verwalteter Geräte

Wenn Sie Geräte nicht während der Ersteinrichtung registriert haben, lesen Sie [dieses Dokument](#) für Anweisungen zur Registrierung eines Geräts bei einem FireSIGHT Management Center.

## Schritt 6: Aktivieren installierter Lizenzen

Bevor Sie eine Funktionslizenz auf Ihrer Appliance verwenden können, müssen Sie sie für jedes verwaltete Gerät aktivieren.

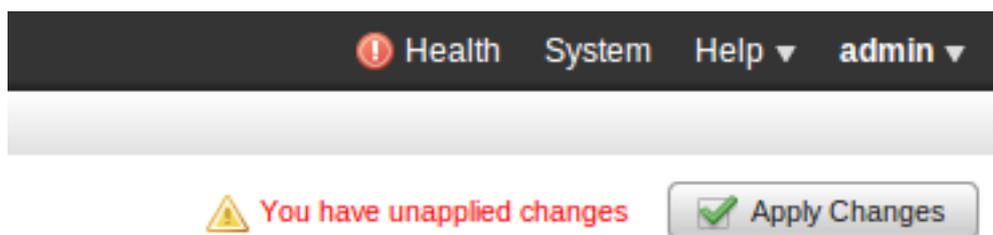
1. Navigieren Sie zur folgenden Seite: **Geräte > Gerätemanagement**.
2. Klicken Sie auf das Gerät, für das Sie die Lizenzen aktivieren möchten, und geben Sie die Registerkarte Gerät ein.
3. Klicken Sie auf **Bearbeiten** (Bleistiftsymbol) neben Lizenz.

### License

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

Aktivieren Sie die erforderlichen Lizenzen für dieses Gerät, und klicken Sie auf **Speichern**.

Beachten Sie die Meldung "*Sie haben nicht angewendete Änderungen vorgenommen*" in der rechten oberen Ecke. Diese Warnung bleibt auch dann aktiv, wenn Sie von der Seite für die Geräteverwaltung weg navigieren, bis Sie auf die Schaltfläche **Änderungen übernehmen** klicken.

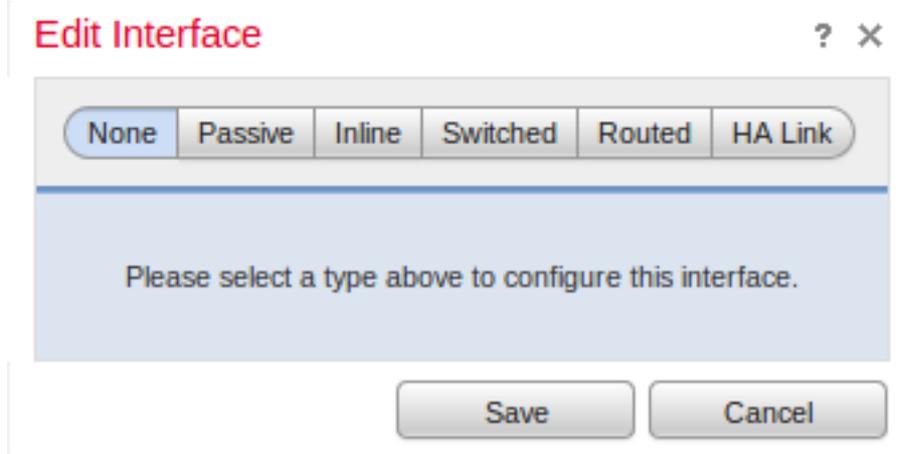


The screenshot shows a dark navigation bar with 'Health', 'System', 'Help', and 'admin' (with a dropdown arrow). Below it, a warning message reads 'You have unapplied changes' next to a yellow triangle icon. To the right is a button with a green checkmark and the text 'Apply Changes'.

## Schritt 7: Konfigurieren von Sensorschnittstellen

1. Navigieren Sie zur folgenden Seite **Geräte > Gerätemanagement**.
2. Klicken Sie auf das Symbol **Bearbeiten** (Bleistift) für den gewünschten Sensor.

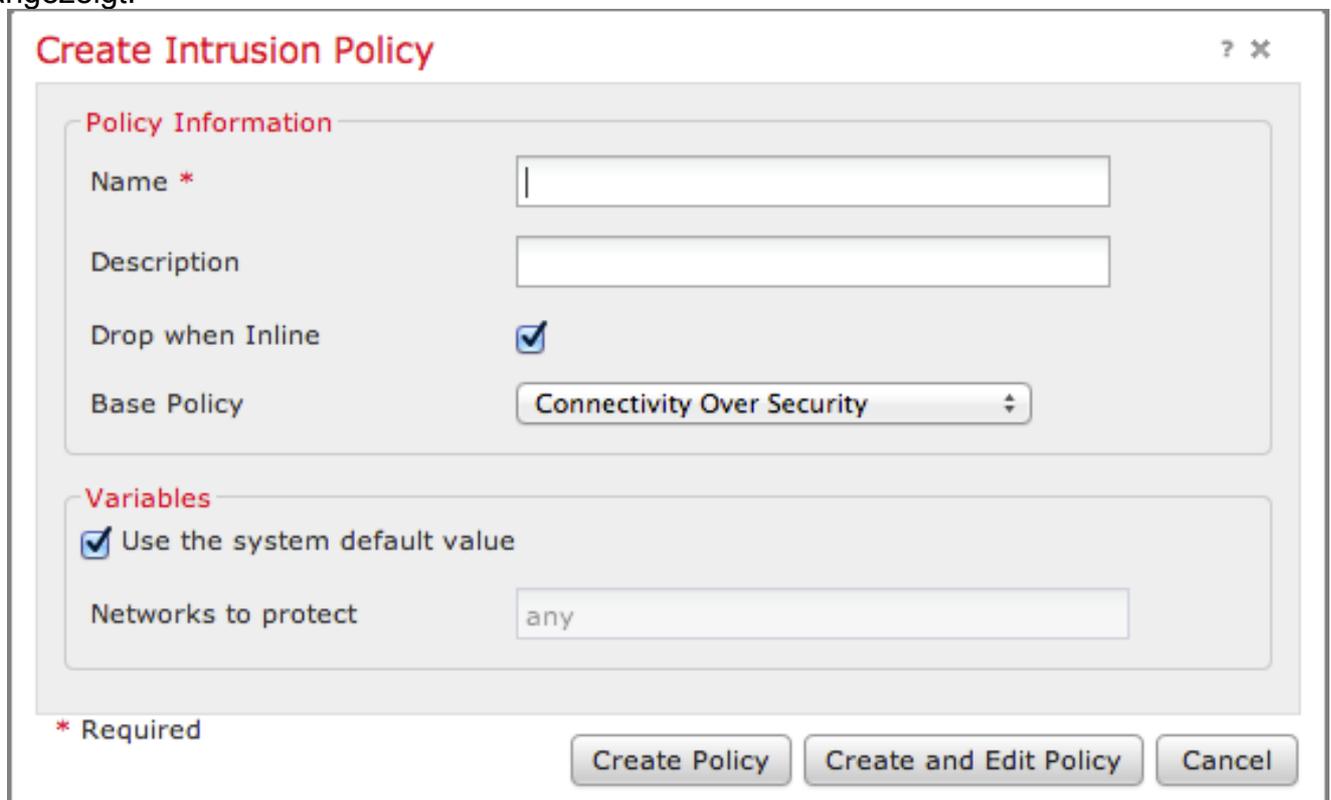
3. Klicken Sie auf der Registerkarte **Schnittstellen** auf das Symbol **Bearbeiten** für die gewünschte Schnittstelle.



Wählen Sie entweder eine passive oder eine Inline-Schnittstellenkonfiguration aus. Switched und Routed Interfaces (Switched und Routed Interfaces) gehen über den Geltungsbereich dieses Artikels hinaus.

## Schritt 8: Konfigurieren der Intrusion Policy

- Navigieren Sie zur folgenden Seite: **Policies > Intrusion > Intrusion Policy (Richtlinien > Sicherheitsrisiken > Zugriffsrichtlinie)**.
- Klicken Sie auf **Create Policy (Richtlinie erstellen)**, und das folgende Dialogfeld wird angezeigt:



Sie müssen einen Namen zuweisen und die zu verwendende Basisrichtlinie definieren. Je nach Bereitstellung können Sie die Option **Drop** wählen, **wenn Inline** aktiviert ist. Definieren Sie die

Netzwerke, die Sie schützen möchten, um Fehlalarme zu reduzieren und die Leistung des Systems zu verbessern.

Wenn Sie auf **Create Policy (Richtlinie erstellen)** klicken, werden Ihre Einstellungen gespeichert und die IPS-Richtlinie erstellt. Wenn Sie Änderungen an der Richtlinie für Sicherheitsrisiken vornehmen möchten, können Sie stattdessen **Richtlinien erstellen und bearbeiten** auswählen.

**Hinweis:** Zugriffsrichtlinien werden als Teil der Zugriffskontrollrichtlinie angewendet. Nach Anwendung einer Richtlinie für Sicherheitsrisiken können alle Änderungen angewendet werden, ohne die gesamte Zugriffskontrollrichtlinie erneut anzuwenden, indem Sie auf die Schaltfläche **Reapply (erneut anwenden)** klicken.

## Schritt 9: Konfiguration und Anwendung einer Zugriffskontrollrichtlinie

1. Navigieren Sie zu **Richtlinien > Zugriffskontrolle**.
2. Klicken Sie auf **Neue Richtlinie**.

**New Access Control Policy** ? X

Name:

Description:

Default Action:  Block all traffic  Intrusion Prevention  Network Discovery

**Targeted Devices**

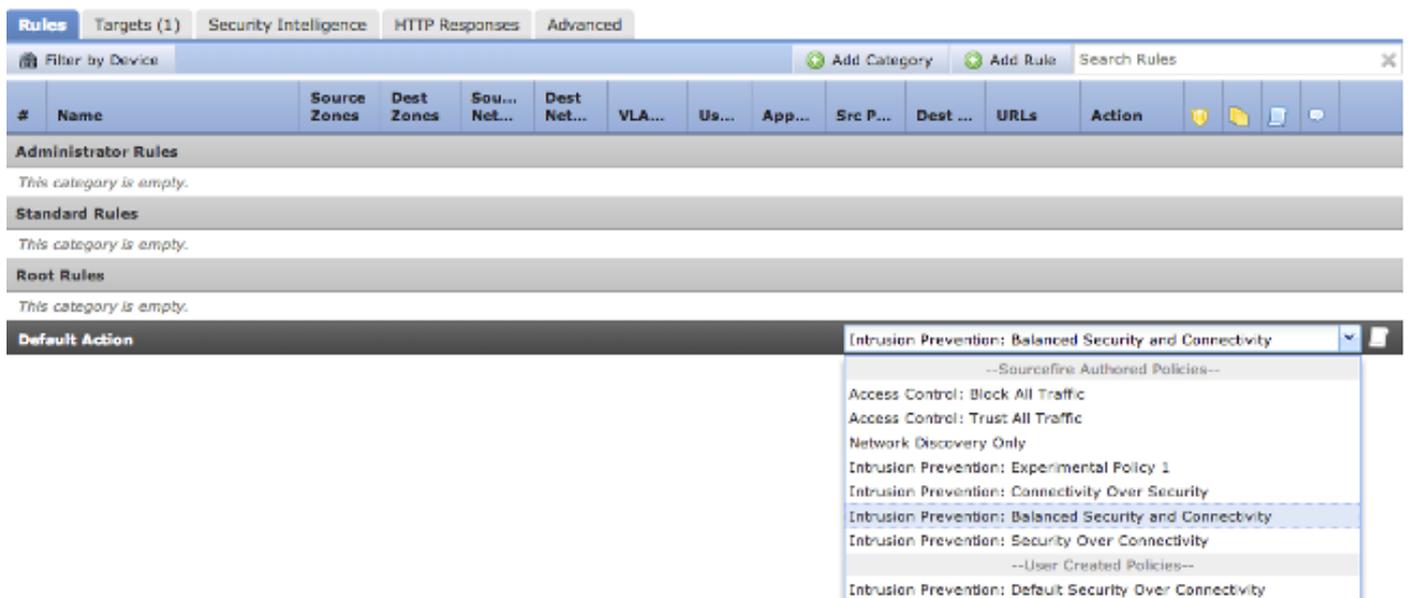
**Available Devices**

**Selected Devices**

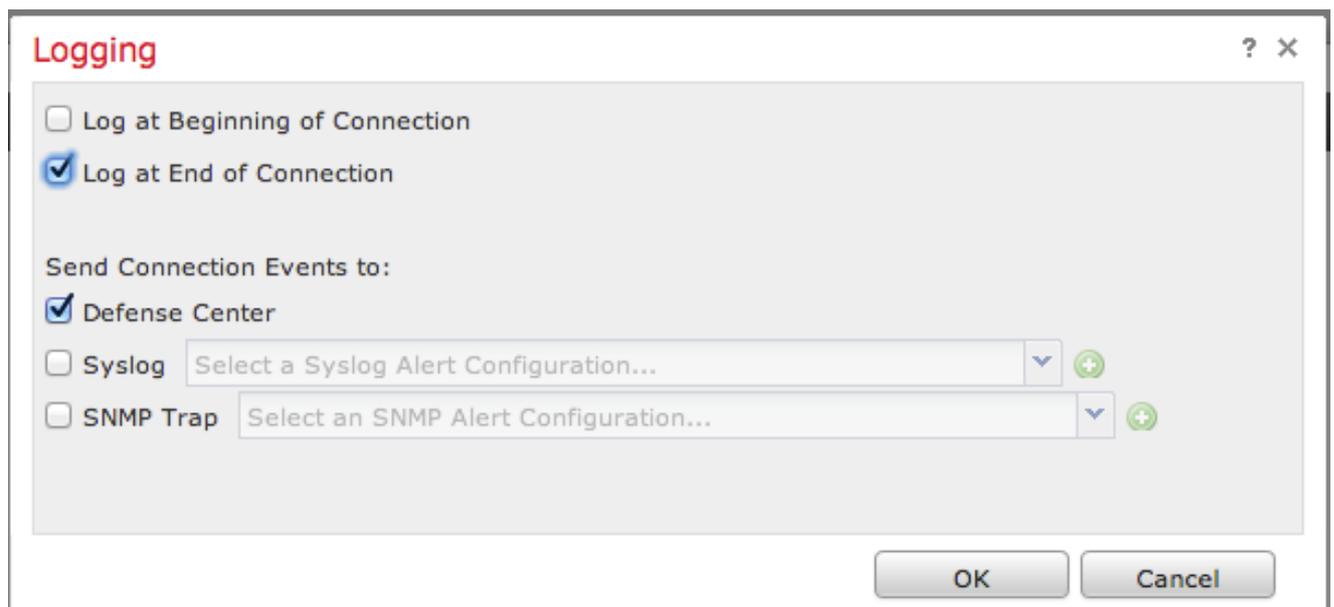
3. Geben Sie einen **Namen** für die Richtlinie und eine **Beschreibung** an.
4. Wählen Sie **Intrusion Prevention** als **Standardaktion** der Zugriffskontrollrichtlinie aus.
5. Wählen Sie schließlich die **Zielgeräte** aus, auf die Sie die Zugriffskontrollrichtlinie anwenden

möchten, und klicken Sie auf **Speichern**.

6. Wählen Sie Ihre Intrusion Policy (Angriffsrichtlinie) für die Standardaktion aus.



7. Die Verbindungsprotokollierung muss aktiviert sein, um Verbindungsereignisse zu generieren. Klicken Sie auf das Dropdown-Menü rechts neben **Standardaktion**.



8. Wählen Sie, ob Verbindungen am Anfang oder am Ende der Verbindung protokolliert werden sollen. Die Ereignisse können im FireSIGHT Management Center, einem Syslog-Speicherort oder über SNMP protokolliert werden.

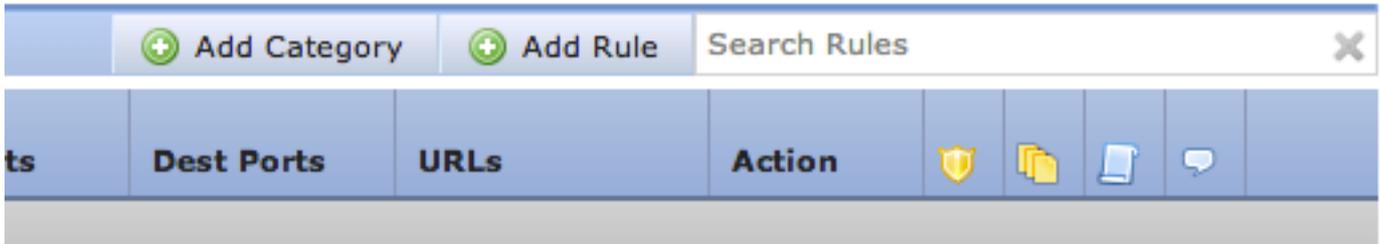
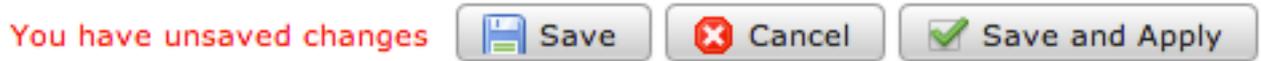
**Hinweis:** Es wird nicht empfohlen, sich an beiden Enden der Verbindung anzumelden, da jede Verbindung (mit Ausnahme der blockierten Verbindungen) zweimal protokolliert wird. Die Protokollierung am Anfang ist nützlich für Verbindungen, die blockiert werden, und die Protokollierung am Ende ist für alle anderen Verbindungen nützlich.

9. Klicken Sie auf **OK**. Beachten Sie, dass sich die Farbe des Protokollierungssymbol geändert hat.

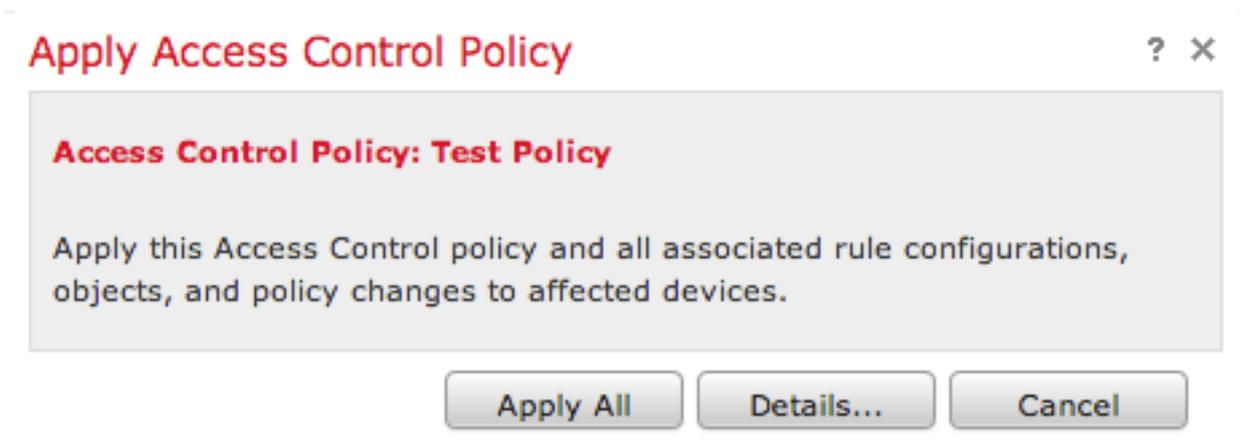
10. Sie können jetzt eine **Zugriffskontrollregel** hinzufügen. Welche Optionen Sie verwenden

können, hängt von der Art der installierten Lizenzen ab.

11. Wenn Sie die Änderungen abgeschlossen haben. Klicken Sie auf die Schaltfläche **Speichern und Übernehmen**. Sie sehen eine Meldung, dass Sie Ihre Richtlinie in der oberen rechten Ecke nicht gespeichert haben, bis Sie auf die Schaltfläche klicken.



Sie können auswählen, nur die Änderungen **speichern** oder auf **Speichern und Übernehmen** klicken. Wenn Sie Letzteres auswählen, wird das folgende Fenster angezeigt.



12. **Wenden Sie All** an, um die Zugriffskontrollrichtlinie und die zugehörigen Zugriffsrichtlinien auf die Zielgeräte anzuwenden.

**Hinweis:** Wenn eine Intrusion Policy zum ersten Mal angewendet wird, kann sie nicht deaktiviert werden.

13. Sie können den Status der Aufgabe überwachen, indem Sie in der oben auf der Seite angezeigten Benachrichtigung auf den Link **Aufgabenstatus** klicken oder zu: **System > Überwachung > Aufgabenstatus**



14. Klicken Sie auf den Link Task Status (Aufgabenstatus), um den Fortschritt der geltenden

Zugriffskontrollrichtlinie zu überwachen.

## 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> 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> Access Control Policy	Access Control Policy applied successfully	2013-07-19 18:26:04	2013-07-19 18:27:12	Completed	

## Schritt 10: Überprüfen, ob das FireSIGHT Management Center Ereignisse empfängt

Nachdem die Zugriffskontrollrichtlinie angewendet wurde, sollten Sie Verbindungsereignisse und abhängig von Ereignissen bei Dateneindringen anzeigen.

## Zusätzliche Empfehlung

Sie können auch die folgenden zusätzlichen Funktionen auf Ihrem System konfigurieren. Details zur Implementierung finden Sie im Benutzerhandbuch.

- Geplante Backups
- Automatische Software-Updates, SRU, VDB und GeoLocation-Downloads/-Installationen.
- Externe Authentifizierung über LDAP oder RADIUS