

FireSIGHT システムの初期設定手順

目次

[概要](#)

[前提条件](#)

[設定](#)

[ステップ 1：初期設定](#)

[ステップ 2：ライセンスのインストール](#)

[ステップ 3：システム ポリシーの適用](#)

[ステップ 4：正常性ポリシーの適用](#)

[ステップ 5：管理対象デバイスの登録](#)

[ステップ 6：インストールされているライセンスの有効化](#)

[ステップ 7：検知インターフェイスの設定](#)

[ステップ 8：侵入ポリシーの設定](#)

[ステップ 9：アクセス コントロール ポリシーの設定と適用](#)

[ステップ 10：FireSIGHT Management Center がイベントを受信するかどうかの検証](#)

[その他の推奨事項](#)

概要

FireSIGHT Management Center または FirePOWER デバイスのイメージ変更が完了したら、システムが完全に機能し、侵入イベントのアラートを生成できるようにするための手順を実行する必要があります（ライセンスのインストール、アプライアンスの登録、正常性ポリシー、システムポリシー、アクセス コントロール ポリシー、侵入ポリシーの適用など）。このドキュメントは、FireSIGHT システムのインストール ガイド ガイドの補足です。

前提条件

このドキュメントは、FireSIGHT システムのインストール ガイドを読んでいることを前提としています。

設定

ステップ 1：初期設定

FireSIGHT Management Center で Web インターフェイスにログインし、次に示すセットアップ ページで初期設定オプションを指定して、セットアップ プロセスを完了する必要があります。こ

のページで、管理者パスワードを変更する必要があります。また、ドメインや DNS サーバなどのネットワーク設定や時刻設定を指定することもできます。

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](#)

任意で、繰り返しルール、位置情報更新、および自動バックアップを設定できます。機能ライセンスもこの時点でインストールできます。

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
------	-------------	---------

このページでは、デバイスを FireSIGHT Management Center に登録し、検出モードを指定することもできます。登録中に選択された検出モードとその他のオプションによって、システムで作成されるデフォルト インターフェイス、インライン セット、およびゾーンだけでなく、管理対象デバイスに最初に適用されるポリシーも決定されます。

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

ステップ 2：ライセンスのインストール

初期設定のページでライセンスをインストールしていない場合は、次の手順に従ってこの作業を実行できます。

- 次のページに移動します： [System] .> [Licenses]
- [Add New License] をクリックします。

Add Feature License

License Key

License

Get License

Verify License

Submit 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.

Return to License Page

ライセンスを受け取っていない場合は、お客様のアカウント担当のセールス担当者にお問い合わせください。

手順 3： システム ポリシーの適用

システム ポリシーは、FireSIGHT Management Center および管理対象デバイス間の時刻同期と認証プロファイルの設定を指定します。 システム ポリシーを設定または適用するには、[System] > [Local] > [System Policy] に移動します。 デフォルトのシステム ポリシーが提供されますが、このデフォルト ポリシーをすべての管理対象デバイスに適用する必要があります。

ステップ 4： 正常性ポリシーの適用

正常性ポリシーは、管理対象デバイスが各自のヘルス ステータスを FireSIGHT Management Center に報告する方法を設定するのに使用されます。 正常性ポリシーを設定または適用するには、[Health Policy] に移動します。 デフォルトの正常性ポリシーが提供されますが、このデフォルト ポリシーをすべての管理対象デバイスに適用する必要があります。

ステップ 5： 管理対象デバイスの登録

初期設定ページでデバイスを登録しなかった場合は、[このドキュメント](#)を読み、FireSIGHT Management Center へのデバイスの登録手順を確認してください。

ステップ 6： インストールされているライセンスの有効化

アプライアンスで機能ライセンスを使用するには、各管理対象デバイスで機能ライセンスを有効にしておく必要があります。

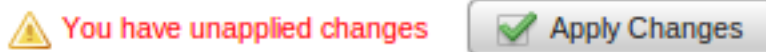
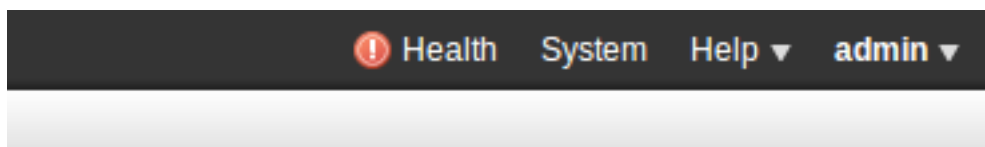
1. 次のページに移動します： [Devices] > [Device Management]
2. ライセンスを有効にするデバイスをクリックし、[Device] タブを表示します。
3. [License] の横の [Edit] (鉛筆アイコン) をクリックします。

License

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

このデバイスに必要なライセンスを有効にし、[Save] をクリックします。

右上隅に「You have unapplied changes」というメッセージが表示されます。この警告は、デバイス管理ページから移動した後でも、[Apply Changes] ボタンをクリックするまではアクティブなままになります。



ステップ 7： 検知インターフェイスの設定

1. [Devices] > [Device Management] ページに移動します。
2. 該当するセンサの [Edit] (鉛筆) アイコンをクリックします。
3. [Interfaces] タブで、該当するインターフェイスの [Edit] アイコンをクリックします。

Edit Interface



None Passive Inline Switched Routed HA Link

Please select a type above to configure this interface.

Save Cancel

パッシブ インターフェイス設定またはインライン インターフェイス設定を選択します。スイッチド インターフェイスおよびルーテッド インターフェイスは、この記事では扱いません。

ステップ 8： 侵入ポリシーの設定

- 次のページに移動します： [Policies] > [Intrusion] > [Intrusion Policy]
- [Create Policy] をクリックします。次のダイアログボックスが表示されます。

Create Intrusion Policy

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

名前を割り当て、使用するベース ポリシーを定義します。導入環境によっては、[Drop when Inline] オプションを有効にできます。誤検出を削減し、システムのパフォーマンスを改善するために保護するネットワークを定義します。

[Create Policy] をクリックすると、設定が保存され、IPS ポリシーが作成されます。侵入ポリシーを変更する場合は、代わりに [Create and Edit Policy] を選択できます。

注: 侵入ポリシーは、アクセスコントロールポリシーの一部として適用されます。 侵入ポリシーの適用後に [Reapply] ボタンをクリックすると、アクセスコントロールポリシー全体を再適用せずに変更を適用できます。

ステップ 9: アクセスコントロールポリシーの設定と適用

1. [Policies] > [Access Control] に移動します。
2. [New Policy] をクリックします。

New Access Control Policy ? X

Name:

Description:

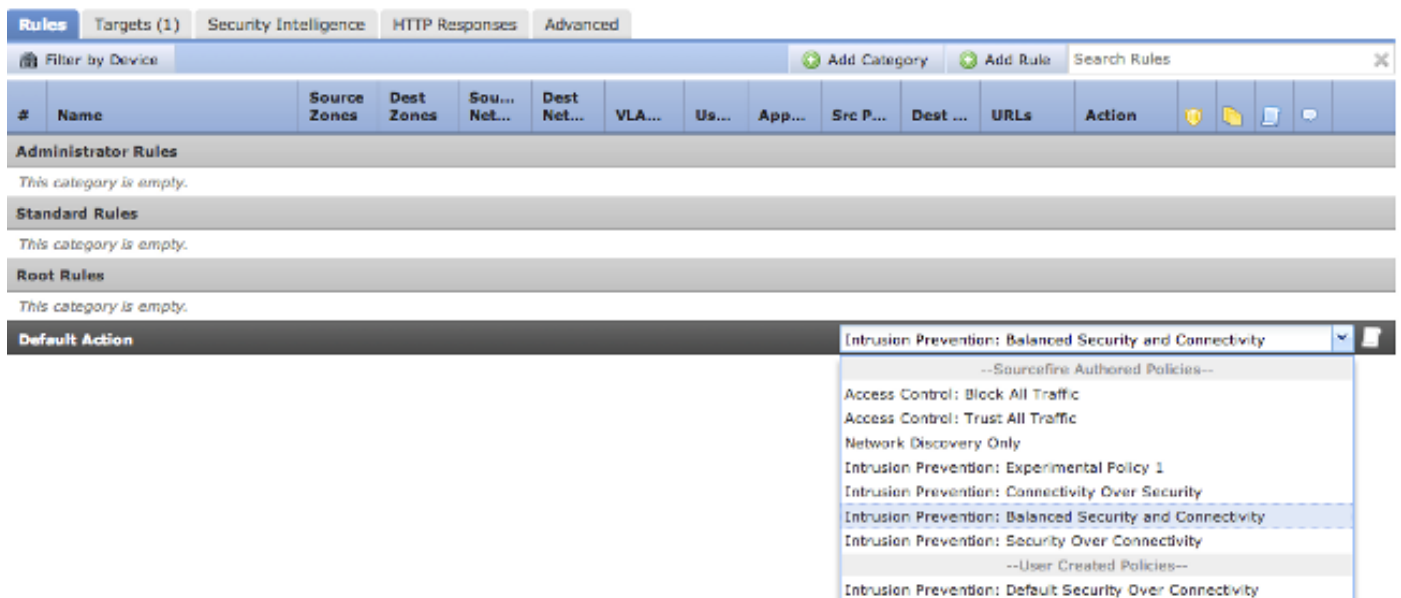
Default Action: Block all traffic Intrusion Prevention Network Discovery

Targeted Devices

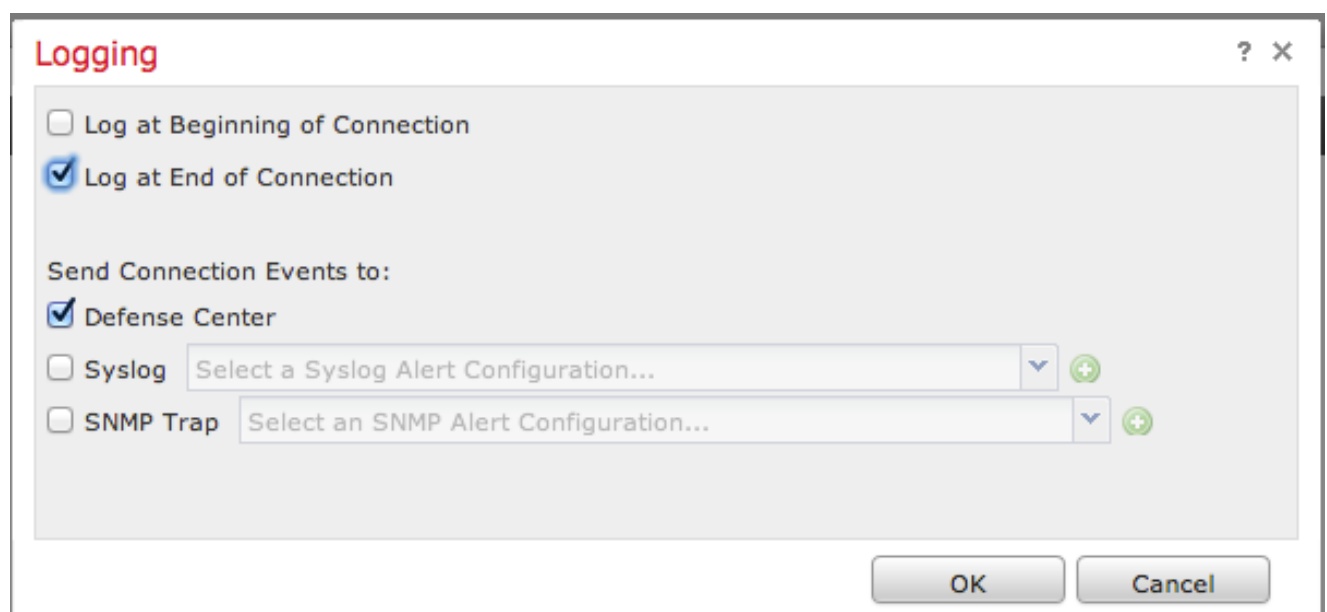
Available Devices

Selected Devices

3. [Name] にポリシーの名前を入力し、[Description] に説明を入力します。
4. [Default Action] で、アクセスコントロールポリシーのデフォルトアクションとして [Intrusion Prevention] を選択します。
5. 最後に [Targeted Devices] で、アクセスコントロールポリシーを適用する対象デバイスを選択し、[Save] をクリックします。
6. デフォルトアクションの侵入ポリシーを選択します。



7. 接続イベントを生成するには、接続ロギングを有効にしておく必要があります。[Default Action] の右側にあるドロップダウンメニューをクリックします。



8. 接続の開始時または終了時に接続をログに記録することを選択します。イベントは FireSIGHT Management Center または Syslog ロケーションでログに記録されるか、または SNMP 経由でログに記録されます。

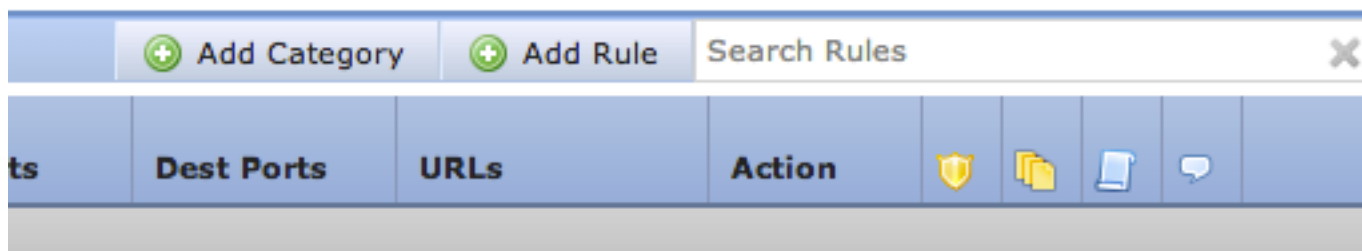
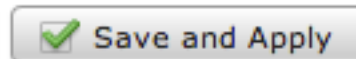
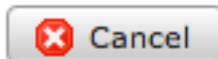
注: 接続の開始時と終了時の両方で記録すると、ブロックされている接続を除くすべての接続が 2 回ログに記録されるため、両側で記録することは推奨されません。開始時に記録すると、ブロックされる接続の場合に役立ち、終了時に記録すると、その他の接続の場合に役立ちます。

9. [OK] をクリックします。ロギング アイコンの色が変化することに注意してください。

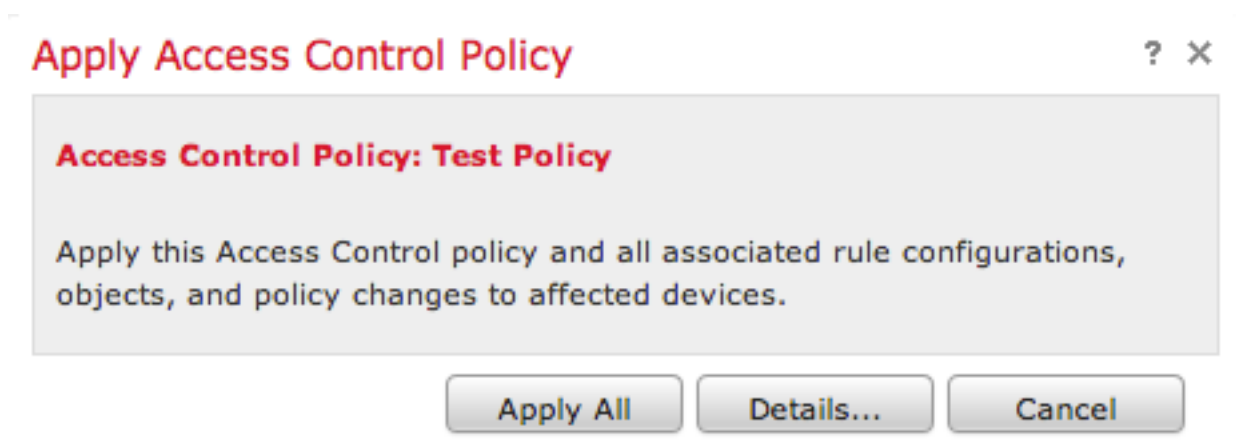
10. この時点でアクセスコントロールルールを追加できます。使用できるオプションは、インストールされているライセンスの種類に応じて異なります。

11. 変更が完了したら、[Save and Apply] ボタンをクリックします。このボタンをクリックするまで、ポリシーの変更が未保存であることを示すメッセージが右上隅に表示されています。

You have unsaved changes



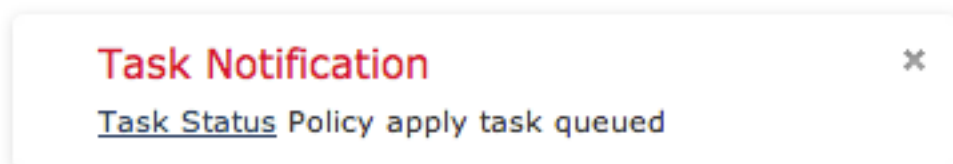
変更を保存するだけか、または保存して適用することを選択できます。後者を選択すると、次のウィンドウが表示されます。



12. [Apply All] は、アクセスコントロール ポリシーと関連するすべての侵入ポリシーをターゲット デバイスに適用します。

注: 侵入ポリシーが初めて適用される場合、このポリシーを選択解除することはできません。

13. タスクのステータスをモニタするには、ページ上部に表示されている通知で [Task Status] リンクをクリックするか、または、[System] > [Monitoring] > [Task Status] に移動します。



14. [Task Status] リンクをクリックして、アクセスコントロール ポリシーの適用の進行状況をモニタします。





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	
 Health Policy apply tasks 0 Running 0 Waiting 1 Completed 0 Retrying 0 Failed					
Health policy apply to appliance [redacted] Health Policy Apply	Health Policy applied successfully	2013-07-19 18:25:39	2013-07-19 18:26:42	Completed	
 Policy apply tasks 0 Running 0 Waiting 3 Completed 0 Retrying 0 Failed					
Apply Default Access Control to [redacted] Access Control Policy	Access Control Policy applied successfully	2013-07-19 18:26:04	2013-07-19 18:27:12	Completed	

ステップ 10 : FireSIGHT Management Center がイベントを受信するかどうかの確認

アクセスコントロール ポリシーの適用が完了すると、接続イベントが表示され、トラフィック侵入イベントを利用できるようになります。

その他の推奨事項

システムでは次の追加機能も設定できます。実装の詳細については、ユーザガイドを参照してください。

- スケジュール バックアップ
- 自動ソフトウェア アップデート、SRU、VDB、および GeoLocation ダウンロード/インストール。
- LDAP または RADIUS を使用した外部認証