

Initial Configuration Steps of FireSIGHT Systems

TAC

Document ID: 118595

Contributed by Nazmul Rajib and Jose Escobar, Cisco TAC Engineers.
Oct 09, 2014

Contents

Introduction

Prerequisite

Configuration

Step 1: Initial Setup

Step 2: Install Licenses

Step 3: Apply the System Policy

Step 4: Apply the Health Policy

Step 5: Register Managed Devices

Step 6: Enable Installed Licenses

Step 7: Configure Sensing Interfaces

Step 8: Configure the Intrusion Policy

Step 9: Configure and Apply an Access Control Policy

Step 10: Verify If the FireSIGHT Management Center Receives Events

Additional Recommendation

Introduction

After you reimage a FireSIGHT Management Center or a FirePOWER Device, you need to complete several steps to make the system fully functional and to generate alerts for intrusion events; such as, installing license, registering the appliances, applying health policy, system policy, access control policy, intrusion policy etc. This document is a supplement to the FireSIGHT System Installation Guide.

Prerequisite

This guide assumes that you have carefully read the FireSIGHT System Installation Guide.

Configuration

Step 1: Initial Setup

On your FireSIGHT Management Center, you must complete the setup process by logging into the web interface and specifying initial configuration options on the setup page, depicted below. On this page, you must change the admin password, and can also specify network settings such as Domain and DNS servers, and the time configuration.

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	<input type="password" value="*****"/>
Confirm	<input type="password" value="*****"/>

Network Settings

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

Protocol	<input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6 <input type="radio"/> Both
IPv4 Management IP	<input type="text"/>
Netmask	<input type="text"/>
IPv4 Default Network Gateway	<input type="text"/>
Hostname	<input type="text"/>
Domain	<input type="text"/>
Primary DNS Server	<input type="text"/>
Secondary DNS Server	<input type="text"/>
Tertiary DNS Server	<input type="text"/>

Time Settings

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

Set My Clock	<input checked="" type="radio"/> Via NTP from <input type="text"/>
	<input type="radio"/> Manually <input type="text" value="2013"/> / <input type="text" value="July"/> / <input type="text" value="19"/> , <input type="text" value="9"/> : <input type="text" value="25"/>
Current Time	2013-07-19 09:25
Set Time Zone	America/New York

You can optionally configure recurring rule and geolocation updates as well as automatic backups. Any feature licenses can also be installed at this point.

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

On this page, you can also register a device to the FireSIGHT Management Center and specify a detection mode. The detection mode and other options you choose during registration determine the default interfaces, inline sets, and zones that the system creates, as well as the policies that it initially applies to managed devices.

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

Step 2: Install Licenses

If you did not install licenses during the initial setup page, you can complete the task by following these steps:

- Navigate to the following page: *System > Licenses*.
- Click on *Add New License*.

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.

If you did not receive a license, contact the Sales Representative of your account.

Step 3: Apply the System Policy

The System Policy specifies the configuration for Authentication Profiles and Time Synchronization between the FireSIGHT Management Center and managed Devices. To configure or Apply the System Policy navigate to *System > Local > System Policy*. A default System Policy is provided but needs to be applied to any managed devices.

Step 4: Apply the Health Policy

The Health Policy is used to configure how managed devices report their health status to the FireSIGHT Management Center. To configure or Apply the Health Policy navigate to *Health > Health Policy*. A default Health Policy is provided but needs to be applied to any managed devices.

Step 5: Register Managed Devices

If you did not register devices during the initial setup page, read this document for instructions on how to register a device to a FireSIGHT Management Center.

Step 6: Enable Installed Licenses

Before you can use any feature license on your appliance, you need to enable it for each managed device.

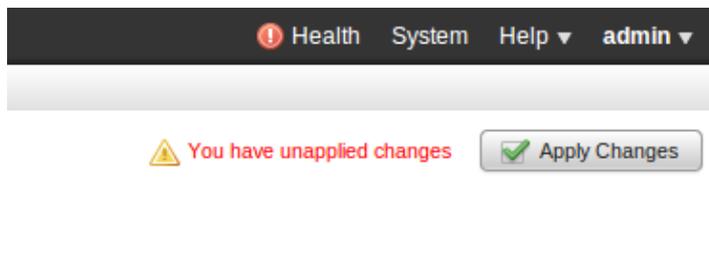
1. Navigate to the following page: *Devices > Device Management*.

2. Click on the device for which you want to enable the licenses and enter the Device tab.
3. Click the *Edit* (pencil icon) next to License.

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

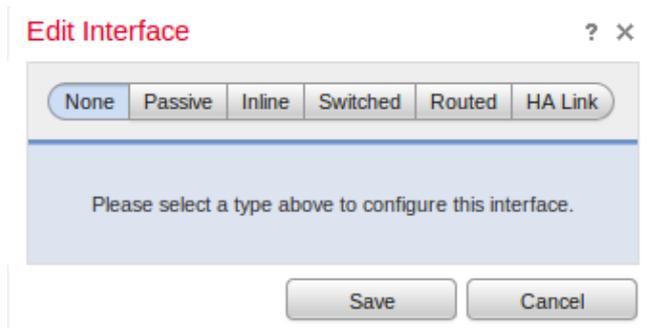
Enable the required licenses for this device and click *Save*.

Notice the message "You have unapplied changes" on the top right corner. This warning remains active even if you navigate away from the device management page until you click the *Apply Changes* button.



Step 7: Configure Sensing Interfaces

1. Navigate to the following page *Devices > Device Management*.
2. Click the *Edit* (pencil) icon for the sensor of your choice.
3. Under the *Interfaces* tab, click the *Edit* icon for the interface of your choice.



Select either a Passive or Inline interface configuration. Switched and Routed interfaces are beyond the scope of this article.

Step 8: Configure the Intrusion Policy

- Navigate to the following page: *Policies > Intrusion > Intrusion Policy*.
- Click on *Create Policy* and the following dialog box is displayed:

Create Intrusion Policy ? x

Policy Information

Name *

Description

Drop when Inline

Base Policy

Variables

Use the system default value

Networks to protect

* Required

You must assign a name and define the base policy to be used. Depending on your deployment you can choose to have the option ***Drop when Inline*** enabled. Define the networks you want to protect to reduce false positives and improve the performance of the system.

Clicking on ***Create Policy*** will save your settings and create the IPS policy. If you want to make any modification to the intrusion policy, you can choose ***Create and Edit Policy*** instead.

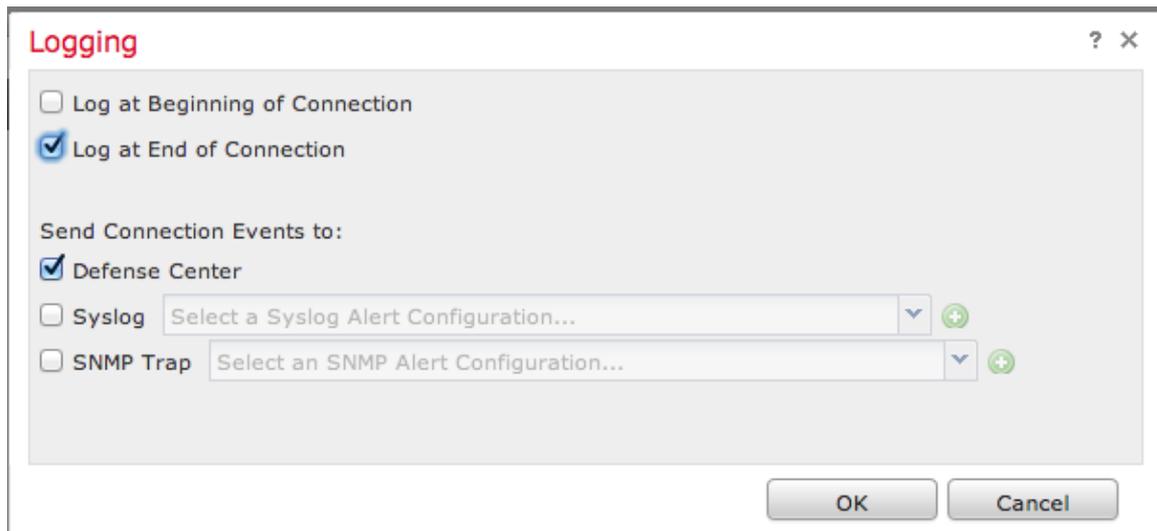
Note: Intrusion policies are applied as part of the Access Control policy. After an Intrusion policy is applied, any modifications can be applied without reapplying the whole Access Control policy by clicking the ***Reapply*** button.

Step 9: Configure and Apply an Access Control Policy

1. Navigate to ***Policies > Access Control***.
2. Click on ***New Policy***.

3. Provide a *Name* for the policy and a *Description*.
4. Select *Intrusion Prevention* as the *Default Action* of the Access Control policy.
5. Finally select the *Targeted Devices* to which you want to apply the access control policy, and click *Save*.
6. Select your Intrusion policy for the default action.

7. Connection logging must be enabled to generate connection events. Click the drop down menu which is right of the *Default Action*.



8. Choose to log connections at either the beginning or the end of the connection. The events can be logged on the FireSIGHT Management Center, a syslog location, or through SNMP.

Note: It is not recommended to log at both ends of the connection because every connection (except blocked connections) will be logged twice. Logging at the beginning is useful for connections that will be blocked, and logging at the end is useful for all other connections.

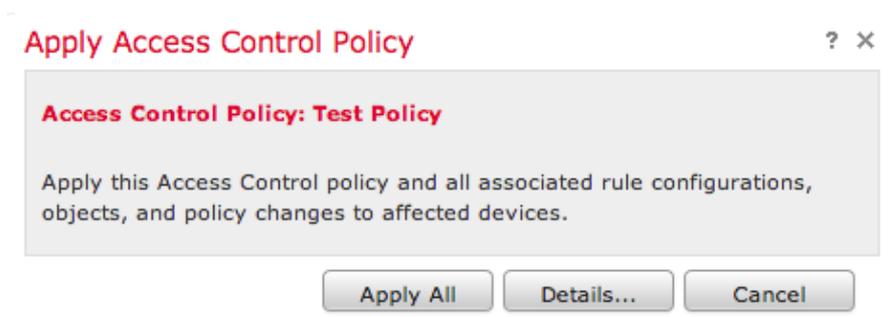
9. Click **OK**. Note that the color of the logging icon has changed.

10. You may add an **Access Control Rule** at this time. The options you can use depend on the type of licenses you have installed.

11. When you are finished making changes, click the **Save and Apply** button. You will notice a message indicating you have unsaved changes on your policy on the upper right corner until the button is clicked.



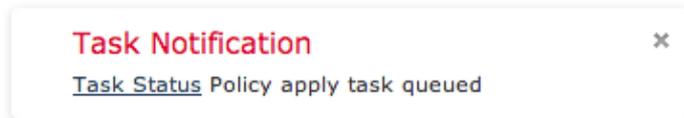
You can choose to only **Save** the changes or click on **Save and Apply**. The following window will appear if you choose the latter.



12. **Apply All** will apply the Access Control policy and any associated Intrusion policy(s) to the targeted devices.

Note: If an intrusion policy will be applied for the first time, it cannot be unselected.

13. You can monitor the status of the task clicking on the **Task Status** link on the notification shown at the top of the page, or by navigating to: **System > Monitoring > Task Status**



14. Click the Task Status link to monitor the progress of the Access Control policy apply.

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

Step 10: Verify If the FireSIGHT Management Center Receives Events

After the Access Control policy apply has completed, you should start seeing connections events and depending on traffic intrusion events.

Additional Recommendation

You can also configure the following additional features on your system. Please refer to the User Guide for implementation details.

- Scheduled backups
- Automatic Software update, SRU, VDB, and GeoLocation downloads/installations.

- External Authentication through LDAP or RADIUS

Updated: Oct 09, 2014

Document ID: 118595
