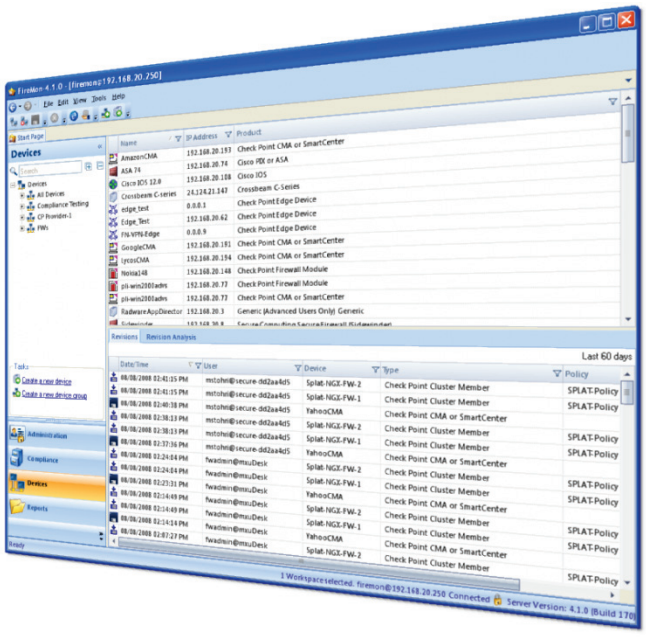
# Getting Started with FireMon eVolution 5.0



Secure Passage, LLC.
8400 W. 110th St, Suite 400
Overland Park, KS 66210
United States of America

# Contents

# 1 Thank You and Introduction

Thank you for purchasing FireMon, the leading Security Operations Management solution by Secure Passage. FireMon is a software product that helps you monitor and manage changes to firewalls, routers, switches and other network security devices so that you can ensure proper device operation.

## About This Guide

This guide is intended for product administrators who are installing FireMon for the first time.

This document assumes you have familiarity with:

- TCP/IP Networking and LAN technology
- Your network and firewall structure
- Administrator permissions and device management knowledge for the devices that you plan to monitor with FireMon

Please complete the chapters in order to prevent installation errors.

## Help

If you encounter any problems while installing FireMon, please contact our Support team. Please provide the following information:

- Your name
- Company
- Version of FireMon
- OS
- Description of the error or issue that you are encountering
- Supporting information like screen shots or error messages

**Telephone**: +1 (913) 948-9570

**Email**: support@firemon.com.

**For FireMon evaluation users only**: please contact us at evals@firemon.com so that your inquiries are routed to the Eval Support team.

## Document History

Please note that this document is usually updated for major releases only.

| Document Name | FireMon Software Version | Changes Made in Document | Date Posted |
|---|---|---|---|
| GettingStarted_FM4-1 | FireMon 4.1.2 | First document draft. | 11/05/2008 |
| GettingStarted_FM4-2 | FireMon 4.2 | Lowercase “l” in Sidewinder configuration command.<br>Addition of port 3193 in the Communication Protocols. | 12/29/2008 |
| GettingStarted_FM5-0 | FireMon 5.0 | Addition of port 8443 in the Communication Protocols<br>Addition of NSM in the Supported Devices table and in the Set Up Device Monitoring section.<br>Addition of special notes throughout the document for evaluation users running FireMon on a VM.<br>Modification of Environment Wizard for Check Point in the Set Up Monitoring section.<br>In GUI requirements, replaced .NET 2.0 framework with .NET 3.5 SP1 framework. | 06/15/2009 |

# 2 FireMon Basics

This chapter introduces you to the main FireMon components, communication and the devices that FireMon monitors.

***Chapter Objectives***

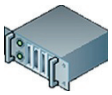
- ✓ Understand the four software components that make up FireMon
- ✓ Learn how FireMon communicates with your devices
- ✓ Learn what devices FireMon monitors

## What is FireMon?

FireMon is a software product that helps you monitor and manage changes to firewalls, routers, switches and other network security devices so that you can ensure proper device operation.

## FireMon Components

The FireMon software consists of four components:



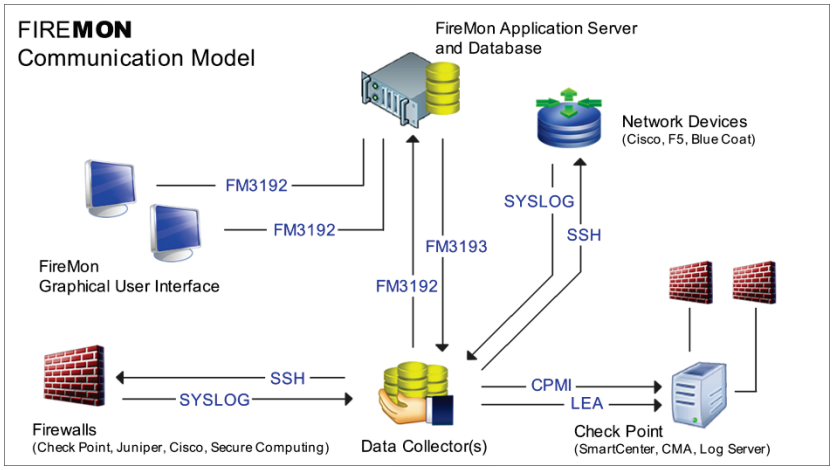
**Application Server (AS)**: Stores the data collected by the Data Collector in the Database. Processes all transactions that occur between the GUI and the Database. The Application Server is installed on a single machine in your enterprise and it must have connectivity with the Data Collector. It is installed on a Linux or Windows platform.

**Database:** Records the data collected by the Data Collector and new data created by users in the GUI. The Database is installed on the Application Server host machine. It is installed on a Linux or Windows platform.

**Data Collector (DC)**: Monitors devices for change. The DC must have connectivity with all network security devices and the Application Server. Multiple DCs can be installed on separate server-class machines for scalability or geographic reasons. It is installed on a Linux or Windows platform.

**Graphical User Interface (GUI)**: Interactive environment for viewing device data stored in the Database. The GUI is installed on the Windows desktop of every user who uses FireMon and must have connectivity with Application Server.

## Communication Model




## Supported Devices

| Manufacturer | Device | Versions |
|---|---|---|
| Cisco | ASA | 7 and later |
| Cisco | Catalyst® OS (CatOS) | 6.1 and later |
| Cisco | IOS® | 11.0 and later |
| Cisco | PIX® | 6.0 and later |
| Cisco | FWSM | 3.0 and later |
| Nokia | IPSO | 3.4 and later |
| Check Point® | FireWall-1® | NG™ FP3 and later |
| Check Point | VPN-1 Edge™ | NGX™ and later |
| Check Point | Provider-1® Multi-Domain Server (MDS) | NG FP3 and later |
| Check Point | Provider-1 Customer Management Add-on (CMA) | NG FP3 and later |
| Check Point | SmartCenter™ | NG FP3 and later |
| Check Point | Log Servers | NG FP3 and later |
| Check Point | SecurePlatform™ | NG FP3 and later |
| Juniper Networks | NetScreen® | 5.0 and later |
| Juniper Networks | Network and Security Manager (NSM) | 2008.1 and later |
| Crossbeam Systems | XOS™ | 8.x and later |
| Crossbeam Systems | COS ™ | 6.x and later |
| Secure Computing | Sidewinder | |

# 3 Install FireMon

This chapter provides the installation processes for Windows and Linux deployments.

**For FireMon evaluation users only**: if you are running an evaluation version of FireMon packaged as a virtual machine, the following installation procedures will not apply. Please refer to the User Center for instructions on installing FireMon.

***Chapter Objectives***

- ✓ Learn system requirements for installing FireMon
- ✓ Install FireMon software

## Installation System Requirements

| Component | HDD | OS Platform |
|---|---|---|
| GUI | 47 MB | **Windows**®: 2003, XP |
| Application Server / Database | 60 MB / 75 MB | **Windows**: 2003, XP<br>**Linux**: Red Hat Enterprise Linux™ 4<br>CentOS Linux 4<br>FireMon Appliance (SPX 120, 250, 500, 502, 504r) |
| Data Collector | 40 MB | **Windows:** 2000, 2003, XP<br>**Linux**: Red Hat Enterprise Linux 4<br>CentOS Linux 4<br>FireMon Appliance (SPX 120, 250, 500, 502, 504r) |

## Installation Options

In most cases, you will install the FireMon Application Server, Database and Data Collector on a single machine. For geographic or scalability reasons, you can install multiple Data Collectors on different machines.

## Install FireMon on Windows

Please complete this process if you are installing the FireMon Application Server on a Windows machine.

### 1. Allocate Space on Your Server

To allocate space on your Windows Application Server machine for processing activities and data, please follow the guidelines listed in the Appendix. If you have sizing questions regarding your organization's system or questions that are not addressed, please email our Support team at support@firemon.com.

### 2. Upgrade to Java 6 (1.6) or later

Download and install Java 6 Update 14 on the Application Server host machine. You can download Java Runtime Environment (JRE) 6 (also known as 1.6) or later, or the latest Java Developer Kit (preferred), which will include JRE 6 or later. If you do not download and install Java 6 manually, the FireMon Server installer will launch a bundled JRE 6 Update 14 for you.

## 3. Install ActivePerl

Download and install ActivePerl by Active State on the Application Server host machine. You can download it for free at www.activestate.com. Be sure to download the ActivePerl Microsoft Installer (MSI), *not* the ActiveState installer (AS package).

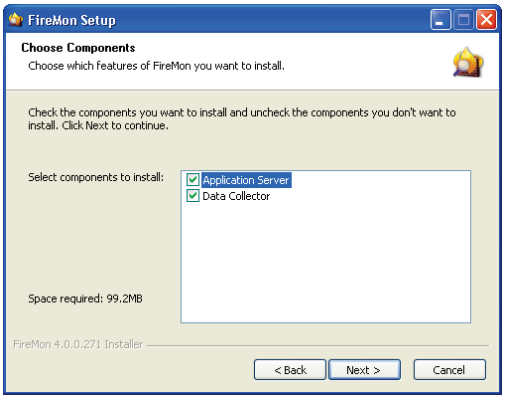
## 4. Download FireMon

1. Log into the User Center at https://usercenter.securepassage.com. Your username and password were emailed to you with your FireMon product license file.
2. Go to **Downloads>Current Downloads**.
3. Download the Application Server installation package.
4. Download the GUI client installation package.

## 5. Install the FireMon Server Components

The installation EXE launches the FireMon Setup Wizard, which installs the Application Server and Database and Data Collector on a single machine in your enterprise. If you have worked with our sales engineers to determine that you need more than one Data Collector, please contact us for an alternate installation procedure.

1. Open the FireMon Server executable file on the machine where you want to install the Data Collector or Application Server and Database. When the Welcome screen appears, click **Next**.
2. Review the terms of the license agreement. If you agree to the terms, click **I Agree**, and then click **Next**.
3. Make sure that both the Application Server and Data Collector check boxes are selected and click **Next**. The Database is automatically installed on the Application Server host machine.
4. Select the installation folder for FireMon and click **Next**.
5. Select the Database installation folder and click **Next**. Shared network drive is not supported.
6. Enter the IP Address of the host machine on which the components will be installed and click **Install**. The IP address should be the same Application Server IP address that you provided to Secure Passage to generate your FireMon product license.




3 – Choose Components

7. When the installation is complete, restart the Application Server and Data Collector services.
    a. In the **Start** menu on the desktop, click **Run**. Then type `services.msc` and click **OK**.
    b. On the right side of the window, right-click the entry "Secure Passage FireMon Data Collector" and select **Restart**. Wait for the service to start before continuing.
    c. On the right side of the window, right-click the entry "Secure Passage FireMon Application Server" and select **Restart**. Wait for the service to start before continuing.

## 6. Install the FireMon GUI Client

Download or copy the GUI Client package to the Windows desktop of any user who will use FireMon. Open the .exe file to run the GUI Client Setup Wizard.

This step can be repeated on the Windows machine of any user who will be using FireMon.

Note that if the .NET 3.5 SP1 framework is not installed on the Windows computer, the GUI Client installer will prompt you to download it from the Microsoft Web site. This step will require an Internet connection and a browser.

## Configure the SPX Appliance for FireMon

Please complete this process if you are configuring an SPX appliance (Linux) for the first time.

Your SPX appliance ships with the latest version of FireMon installed. However, the appliance must be configured for FireMon to work in your system. All appliance configuration is done at the command line.

It is assumed that you have already physically installed the Appliance.

### Required Information

Before you begin, please make sure that you can provide the required information.

#### Required Information

1. The hostname of the device, including domain name.
2. The interfaces that should be active.
3. The static IP address and netmask for the primary network interface.
4. Desired password for the “root” user, which gives root console access.
5. Desired password for the “firemon” user, which gives CLI access.

#### Recommended Information

1. Default gateway IP address.
2. DNS server IP address.

### 1. Connect a console to the Appliance

The Appliance is configured to accept console connections through the VGA and keyboard ports, or through a serial console.

The serial console is configured with the following settings:

- 9600 baud
- No parity
- 8 bits
- Vt100 emulation
- No flow control

1. If you have not already done so, connect a console to the appliance:
    A. Make sure that power to the appliance is off.
    B. Connect the appliance to the network by plugging an Ethernet cable into eth0.
    C. Plug the following components into the proper ports on the back of the appliance:
        A. Keyboard – USB or PS2, and VGA monitor, or
        B. Serial console

2. Connect the power cord to the appliance and plug into a power supply.

## 2. On First Boot, Run the Configuration Wizard

The first time you boot the appliance, a configuration wizard will run.

1. Turn on the appliance.
2. When prompted by the configuration wizard, enter the information that you gathered earlier.
3. When prompted by the configuration wizard, confirm the changes.
4. After the wizard confirms that the changes have been applied, the appliance will restart. This step causes the changes to take effect.

## 3. Test the Configuration

1. Log in with the username “firemon” and the password that you created in the configuration wizard.
   Once the Appliance has been configured, it will accept SSH connections for logins.
2. Test the appliance configuration by verifying the status of the Application Server and Data Collector. Type the command **firemon status**.

   The output will be similar to the following:

   ```
   JAS is running…
   DataCollector is running
   ```

   The **firemon** command also provides stop and start functionality for the FireMon servers.

## 4. Verify Communication

Next, verify the connection between the Application Server and Data Collector.

1. Type the command **show firemon dc connections**.

   The output will be similar to:

   FireMon DC is accepting connections on:*192.168.20.250:3193*

   FireMon JAS<->DC Connections:*192.168.20.250:33488->192.168.20.250.3192*

   Where *192.168.20.250:XXXX* is specific to your Data Collector or Application Server.

2. Next, confirm that the appliance can connect to the devices that you want to monitor. Type the **ping** command from the Data Collector to verify connectivity.

   *Example*:

   firemon@>**ping *192.168.20.192***
   PING 192.168.20.102 (192.168.20.192) 56(84) bytes of data.
   64 bytes from 192.168.20.192: icmp_seq=0 ttl=255 time=2.72 ms
   64 bytes from 192.168.20.192: icmp_seq=1 ttl=255 time=1.16 ms
   64 bytes from 192.168.20.192: icmp_seq=2 ttl=255 time=1.53 ms
   64 bytes from 192.168.20.192: icmp_seq=3 ttl=255 time=1.23 ms

   --- 192.168.20.192 ping statistics ---
   4 packets transmitted, 4 received, 0% packet loss, time 3007ms
   rtt min/avg/max/mdev = 1.167/1.663/2.721/0.626 ms, pipe 2

   In this example, we confirmed that the Appliance is able to communicate with the device at *192.168.20.192* (in this case, a device running a Check Point management server).

## 5. Install the FireMon GUI Client

1. Download the FireMon GUI client. This step requires and Internet connection and a browser. You can download the GUI client package from the User Center at https://usercenter.securepassage.com. Your username and password were emailed to your organization with your FireMon product license file.

2. Install the GUI Client on a Windows machine. Open the client-EXE file to run the FireMon GUI Setup Wizard.
   This step can be repeated on the Windows machine of any user who will be using FireMon.

   Note that if the .NET 3.5 SP1 framework is not installed on the Windows computer, the GUI Client installer will prompt you to download it from the Microsoft Web site.

# 4 Set Up Device Monitoring

## Before You Begin

Please take a moment to complete the following steps.

### 1. Locate Your FireMon Product License

Copy the FireMon product license file to the Windows machine that you will use to log into the GUI.

### 2. Gather Required Information

Please have the following information available. You will enter it in the GUI shortly after login:

- A username, password and email address for a new FireMon GUI Administrator account. You will create this account after you log in.
- Mail server or Syslog server settings. FireMon sends Notifications via your mail server or Syslog server. Please provide settings for the method you want to use. Additionally, email settings are required if you want to schedule reports in FireMon.

### 3. Complete the Device Worksheet

Please take a moment to complete the Device Worksheet in the Appendix. The information that you provide will quicken the setup process.

***Chapter Objectives***

- ✓ Pre-configure the devices that you want to monitor
- ✓ Log into the GUI for the first time
- ✓ Enter basic application settings necessary to run FireMon
- ✓ Add devices to FireMon
- ✓ Verify communication with monitored devices

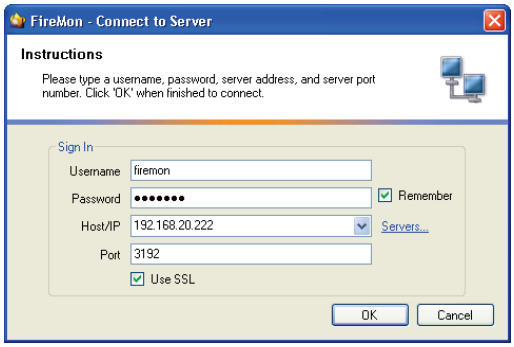
## Step 1: Run the First Run Wizard

1. Open the FireMon GUI.

2. In the login window, type in the following information for your Application Server and click **OK**:
   - Username: firemon
   - Password: firemon
   - Host/IP: for your Application Server
   - Port: 3192 (default)

   **Note**: if you are running an evaluation version of FireMon as a virtual machine (VM), the Host/IP is the same as the IP address of the VM running FireMon.

3. Upon successful login, the status bar will show you are “Connected” and the First Run Wizard will open in a new window.




2 - Login window

4. Complete the First Run Wizard by entering the required information that you gathered earlier. Make sure that you upload a FireMon product license. You cannot complete monitoring setup without a valid product license.

5. The First Run Wizard ends with the Set Up Monitoring screen. Select **Yes** and then click **Next** to exit the First Run Wizard and begin adding devices.

6. The First Run Wizard closes and the New Device window opens. Continue to the Step 2: Add Devices section.

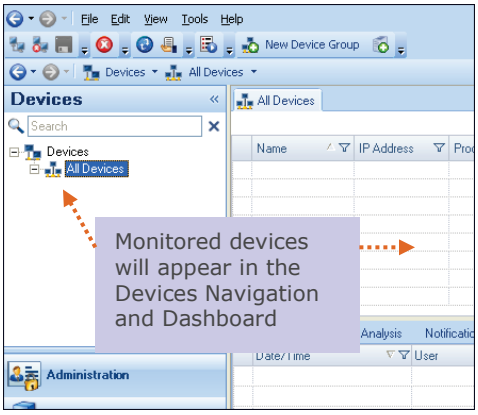
   **Note**: if are unable to set up monitoring now, you can begin later by clicking the **Create a New Device** text link in the **Devices** Navigation. The New Device window opens, and you can continue to Step 2: Add Devices.

   Please note that until you set up monitoring, most of the FireMon features, including configuration retrieval and analysis, will be unavailable.

## Step 2: Add Devices

In this step you will configure the devices that you want to monitor and add representations of those devices in FireMon GUI. The processes listed here are completed both on your device, usually at the command line or through an administration tool, and in the Devices section of the FireMon GUI.

Once the device properties are saved, the names of your monitored devices will be viewable in the **Devices** Navigation and in the FireMon Dashboards.



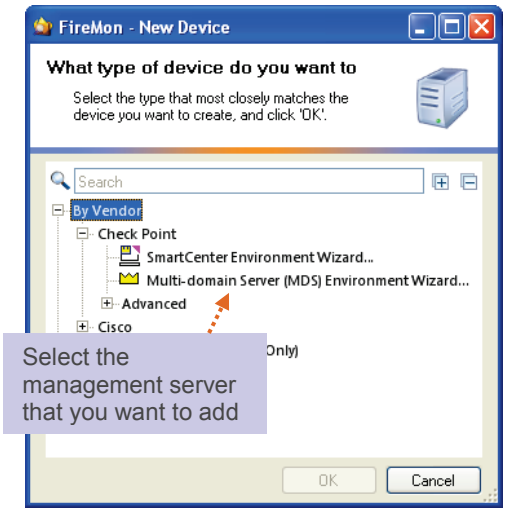

Devices Navigation and Dashboard

Find instructions for your device vendor on the following pages:

## Check Point

### Step 1: Set Up Configuration and Log Retrieval

FireMon's Environment Wizard for Check Point enables you to add some or all Check Point devices that are managed by a single MDS, CMA or SmartCenter. FireMon detects all of the associated firewalls, management servers and log servers, and adds them for you at one time. You can run the Environment Wizard any time that you want to automatically detect and add new devices to FireMon.




New Device Window

1. In the New Device window in the FireMon GUI, click one of the following devices and click **OK**:

   - **Multi-Domain Server (MDS)** Environment Wizard if you want to add all modules managed by an MDS, including CMAs, in a Provider-1 environment.
   - **SmartCenter** Environment Wizard if you have a SmartCenter. You can add all modules managed by a SmartCenter.

2. The Check Point Environment Wizard opens.

3. On this screen, complete the steps that will enable FireMon to communicate with your management server. Then click **Next**:

   1. **Select a Data Collector**: the IP address of the Data Collector that will monitor this management server.

   **Note**: if you are running the evaluation version of FireMon packaged as a virtual machine (VM), the Data Collector IP address is the same as the IP address of the VM running FireMon.

   2. **Add FireMon Data Collector IP address as a GUI Client** on your management server.

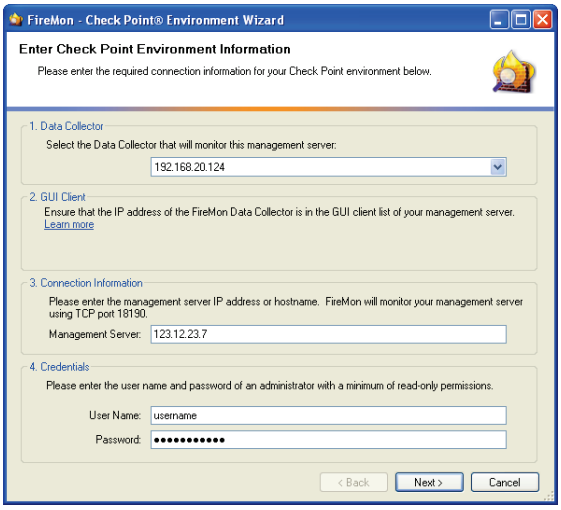
   On a SmartCenter Server, use the Configuration Tool *cpconfig* to add the Data Collector IP address to the GUI client list.

   In a Provider-1 environment, use the *mdsconfig* utility on the MDS to add the Data Collector IP address to the GUI client list. The GUI client entry must also have the proper Customers assigned to it in order to access the CMAs.

   **Note**: this step is required only once on each management server.

   3. **Enter the hostname or IP address of the management server.**

   FireMon uses TCP port 18190 to retrieve configurations from the management server.




Check Point Environment Wizard

4. **Enter credentials.**

   **Username**: the username of an administrator account on the management server. This can be an existing account or a new read-only account that you create for the Data Collector.

   **Password**: the password of an administrator account on the management server. This can be an existing account or a new read-only account that you create for the Data Collector.

4. FireMon verifies communication with the management server. Click **Next**.

5. The Rule Usage Setup screen appears.

6. FireMon uses log data as the foundation of the Rule Usage Analysis feature. FireMon must use Secure Internal Communication (SIC) to communicate with Check Point log servers. To use SIC, an OPSEC application object for FireMon must be created in the management server's database and the resulting certificate retrieved.

   Select **Automatic** and click **Next** to let FireMon create this object automatically for you using CPRA.

   This selection requires one-time use of a read-write administrator login on the management server and that you open port 18210 on the Application Server host.

   **Other options**

   - Select **Manual** if:
     - You have already created the OPSEC object or you plant to create it
     - You cannot enable CPRA
     - You cannot provide a read-write administrator login

       Then see the Alternate Scenarios section in the Appendix.

   - Select **Configure Later** if you want to set up log collection later. Then skip to step 17.

   **Note**: Rule Usage Analysis features will be unavailable until the OPSEC application object is created and SIC certificate is retrieved.

   **Note**: it is assumed that you have enabled logging (in SmartDashboard) for each rule for which you expect rule usage.

7. The “CPRA Requirements” screen appears.

8. On the Application Server host, make sure that port 18210 is open. FireMon will use this port to automatically create the OPSEC application object that will represent the FireMon Data Collector.

9. On your management server, enable Check Point Roaming Administrator (CPRA):

   A. **On NGX (and NG AI up to NG FP3)**:
      1. Log into SmartDashboard™.
      2. Go to **Policy>Global Properties**.
      3. Select **OPSEC** in the left pane and select **Allow remote registration of OPSEC products**.

   B. **On NG FP3 and later:**
      Add the file cpra.conf to the $FWDIR/conf directory on the management server. This file should contain the line:
      `allow_remote_ra=yes`.

      You do not need to restart the management server after this file is added.

10. Make sure that all users with Read/Write permissions are logged out of the policy editor associated with this management server. OPSEC object creation will fail if anyone with Read/Write permissions is logged into a policy editor.

11. On the “CPRA Requirements” screen in the FireMon GUI, click **Next**.
12. The “CPRA” screen appears.
13. Enter the following information:

    **Username**: The username for a Check Point administrator account with Read/Write permissions

    **Password**: The password for a Check Point administrator account with Read/Write permissions

    **Network Object Name**: The name of the OPSEC application object as you want to see it in the management server

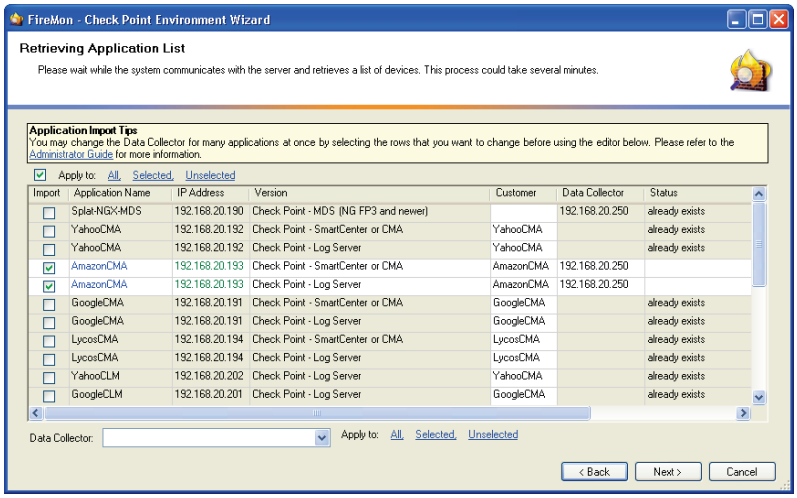
    **OPSEC Application Name**: The name of the OPSEC application associated with the Network Object, as you want to see it in the management server

16. Click **Next.** FireMon will create the object and retrieve the SIC certificate.

**Caution**: If all users with read/write access are not logged out of SmartDashboard, an error will appear indicating that object creation has failed.

17. The Application List screen appears. This screen displays a list of all devices managed by the MDS, CMAs or SmartCenter, including:
    - The MDS and CMAs or SmartCenter
    - Clusters
    - Cluster Members
    - FireWall Modules

18. Review the available information and make changes as necessary:




Application List

### *Device Information*

**Import**

This check box indicates the devices that you want to import. By default, all applications will be selected for import unless they already exist in FireMon.

Clear the check boxes of any devices that you do not want to import.

**Note**: OS's that run the application are not added as "devices." After the Environment Wizard is finished, you must select the OS's as properties for Check Point devices. See instructions for adding your device vendor in this document, or the Device Properties section for your vendor in the Administrator's Guide.

**Note**: To use FireMon's Rule Usage Analysis feature, you must allow FireMon to import representations of your Log Servers. Log servers that log to a management server will appear in the device properties for your CMA or SmartCenter; they will not appear in the GUI as separate devices.

19. Click **Next** to add the devices to FireMon.

20. When FireMon has finished adding your devices, click **Finish** to close the Wizard.

## Step 2: Verify Communication

To verify that FireMon can retrieve configurations and usage data from the device :

1. In SmartDashboard, install the Check Point database to the management server and the log server. This action makes the OPSEC certificate active, so it is imperative that you complete this step.

2. In SmartDashboard, push a policy to the FireWall Modules. This step is necessary for FireMon to associate logs with the correct policy and objects for Usage Analysis.

   **Note**: If this step cannot be completed now, complete a Policy Save in SmartDashboard and continue to step 3. After you push a policy, return to this section and complete steps 7-9.

3. FireMon retrieves the policy.

4. In the Devices Navigation in the FireMon GUI click **All Devices**.

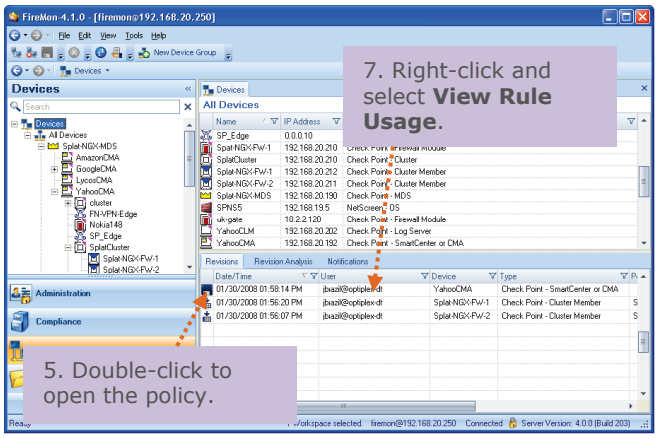
5. Double-click the record of the policy save in the **Revisions** tab.

6. The policy opens in a new tab. At this point, communication with the device has been verified.

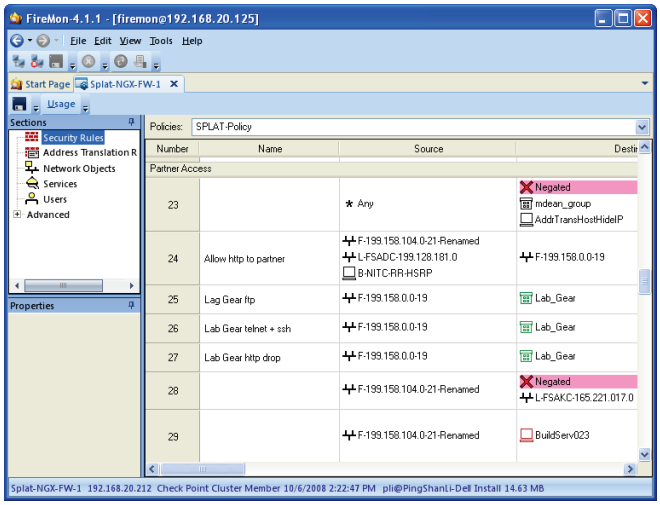
7. To verify usage collection, make sure that you have pushed a policy to the Firewall Modules. Then, wait for the minimum Log Update Interval to pass (default is 10 minutes). Go to the Devices Navigation in the FireMon GUI and click **All Devices**.

8. Right-click the newly retrieved configuration in the **Revisions** tab and select View Rule Usage.

9. Rule Usage Data opens in a new tab.




All Devices

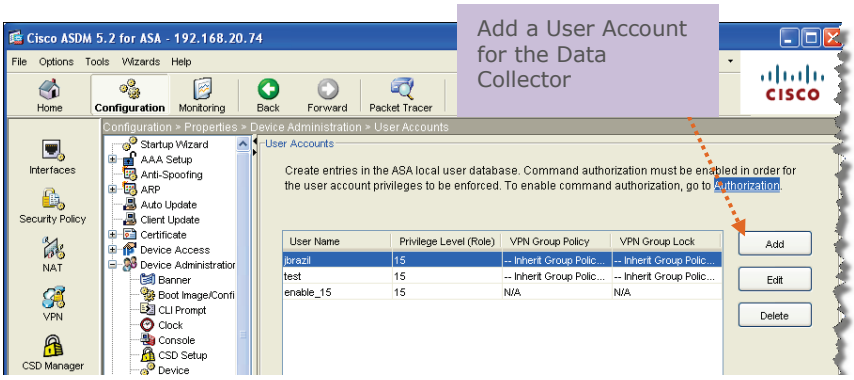


Check Point Policy in FireMon

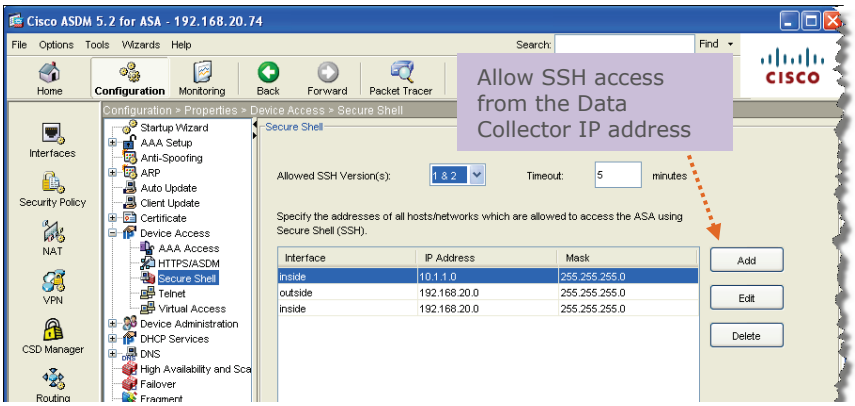
## Cisco

### Step 1: Configure Devices and FireMon Properties

1. Add a user account for the FireMon Data Collector with level 15 permissions. Then write down the username and password. You will need this information for a later step. Remember to enable Authorization.
2. Enable SSH access from the Data Collector IP address.
3. Set the FireMon Data Collector as a Syslog logging server on the Cisco device. Ensure that the Syslog Logging Level is set at a notification level of "informational."
4. If you expect to have ACL traffic, make sure that the keyword “log” is at the end of each ACE. This step is necessary if you want to use the Rule Usage Analysis features in FireMon.




Cisco ASDM | User Accounts




Cisco ASDM | Secure Shell

4. In the New Device window in the FireMon GUI, select the device that you want to add and click **OK**:
5. Enter the device properties:

   **Name** as you want to see it in FireMon.

   **IP Address** of the device (required if you are not using a DNS name).

   **DNS Name** of the device (required if you are not using an IP address).

   **Data Collector** that will retrieve data.

   **Licensed**: select this check box if your FireMon product license includes this device

   **User name**: the user name that you created for the Data Collector earlier.

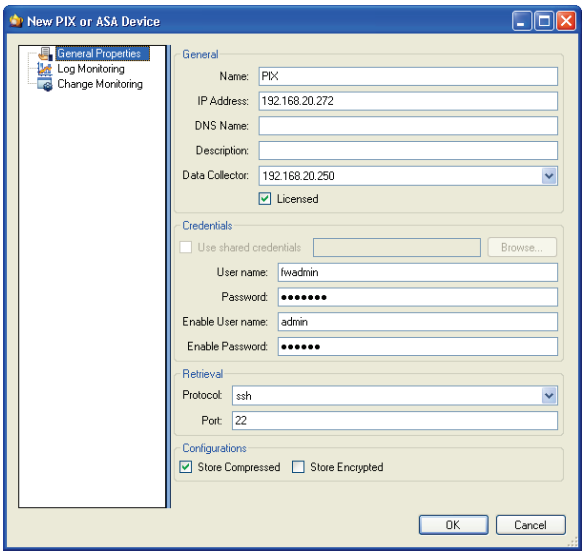
   **Password:** the user name that you created for the Data Collector earlier.

   **Enable User name**: the user name that is used to log into "enable" or EXEC mode.

   **Enable Password**: the password that is used to log into "enable" or EXEC mode.

   **Protocol**: the communication program used between FireMon and the monitored device

   **Port**: the endpoint on the monitored device from which FireMon uses the specified protocol to retrieve device data

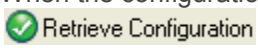



Cisco PIX Properties

2. *For PIX, ASA and FWSM only*: click **Log Monitoring** and verify that the **Monitor Log Data** check box is selected. This step is necessary to enable Rule Usage Analysis for firewalls.
3. *For PIX 6.3.0 and earlier only:* select the **Use legacy log matching** check box on the Log Monitoring screen.
4. Click **OK**.
5. The Device appears in the Devices Navigation.

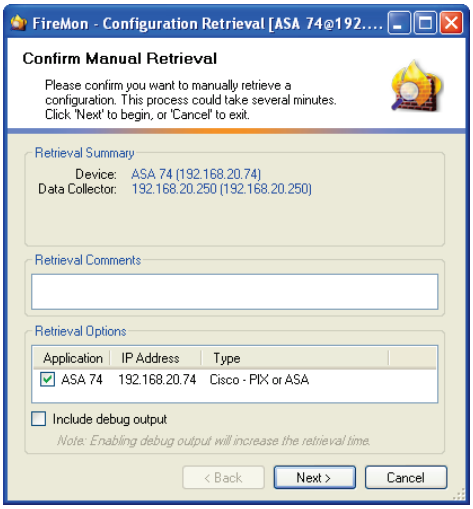
## Step 2: Verify Communication

To verify that FireMon can communicate with the new device, manually retrieve a configuration.

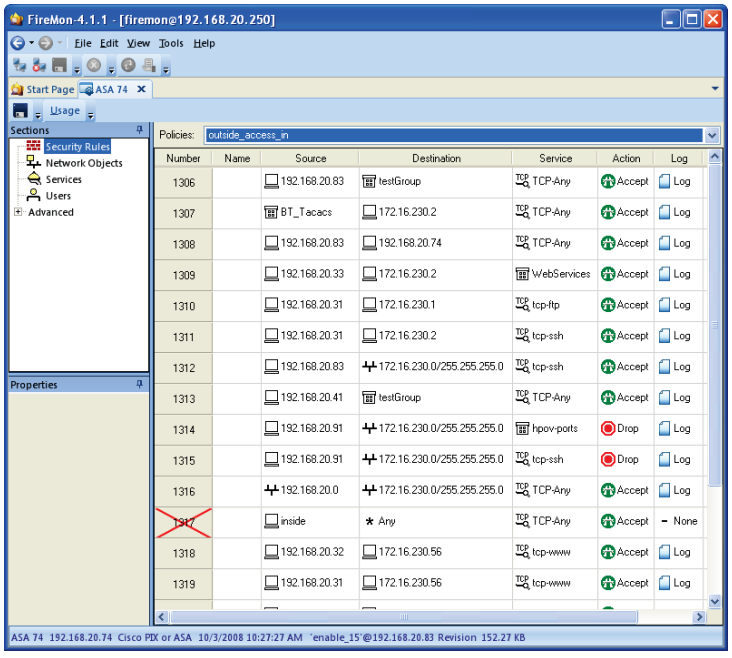
1. In the **Devices** Navigation, right-click the device you just created and select **Retrieve Configuration**.
2. The Configuration Retrieval Wizard opens.
3. Click **Next**.
4. When the configuration is retrieved, a green check mark 

will appear. Click **Finish** to open the configuration.

   **Note**: the configuration display varies according to device type.




Manual Configuration Retrieval




Cisco ASA Policy

## Juniper Networks

### Step 1: Configure Devices and FireMon Properties

1. Enable Syslog Messages on your NetScreen device:

   A. In your NetScreen Administration Tool, go to **Configuration>Report Settings>Syslog**.

   B. Enable Syslog messages by selecting the **Enable Syslog Messages** check box.

   C. Select the **Source Interface** that will communicate with the FireMon Data Collector. On your system, this interface might be named “management” or something similar.

   D. In the **IP/Hostname** field of the Syslog servers section, enter the IP Address of the Data Collector.

   E. In the Port field, enter **514**.

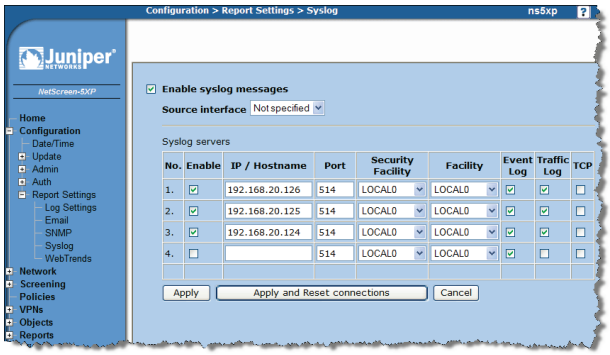
   F. In the **Security Facility** and **Facility** drop-down lists, select the option that enables the FireMon Data Collector to collect all Syslog messages.

   G. Select the **Event Log** check box, enabling FireMon to retrieve configurations.

   H. Select the **Traffic Log** check box, enabling FireMon to collect rule usage data.

   I. Select the **Enable** check box for the Data Collector Syslog server.

   J. Click **Apply**.




Juniper NetScreen 5XP

2. Create an administrator account for the FireMon Data Collector on the NSM. If FireMon will be monitoring NetScreen ScreenOS devices only (with no NSM), please create this account on your NetScreen device. Please see the Administrators’ Guide for information adding a NetScreen ScreenOS device only.

   A. In the NSM, go to the **Administrator** tab and click the **Add** icon.

   B. The New Admin dialog box opens.

   C. In the **General** tab, enter a name for the FireMon Data Collector.

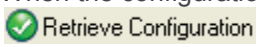
   D. The **Authorization** tab, enter authentication information for the Data Collector.

   E. Write down this account information. You will need it for a later step.

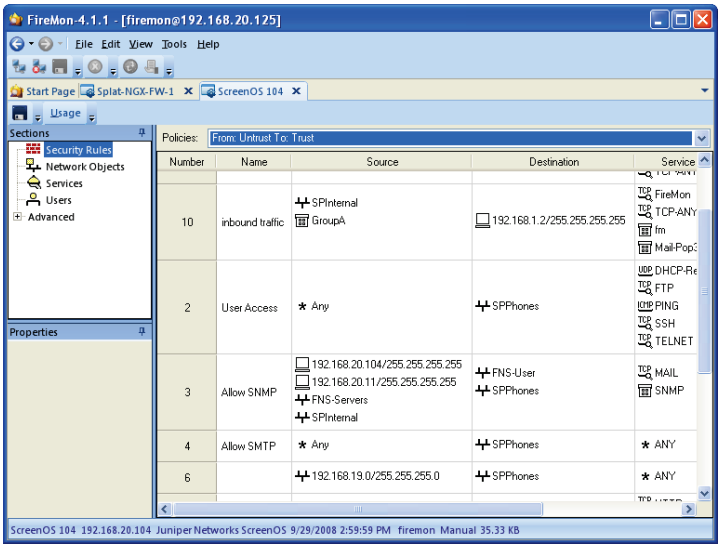
3. In the New Device window in the FireMon GUI, click **NSM** and click **OK.**
4. The Network and Security Manager Setup window opens.
5. Enter the following information and click **Next**:
   - IP Address: address of the NSM
   - Port: the default port is 8443
   - Username: the username that you created for the FireMon Data Collector
   - Password: the password that you created for the FireMon Data Collector
   - Confirm Password
   - Data Collector: the FireMon Data Collector that will monitor this device
6. FireMon adds the NSM and all of the ScreenOS devices that it manages. The devices appear in the Devices Navigation.

## Step 2: Verify Communication

To verify that FireMon can communicate with the NetScreen device, manually retrieve a configuration from a NetScreen device.

1. In the **Devices** Navigation, right-click the device and select **Retrieve Configuration**.
2. The Configuration Retrieval Wizard opens.
3. Click **Next**.
4. When the configuration is retrieved, a green check mark 

will appear. Click **Finish** to open the configuration.




Screen OS Configuration

## Crossbeam

### Step1: Configure Devices and FireMon Properties

1. On your Crossbeam device, add the FireMon Data Collector as a Logging Server. The following logging settings apply: Monitor Level 4, Logging Level 7, Log Level Name 7.
2. On your Crossbeam device, create an Administrator account for the FireMon Data Collector. This should be a read-only account. Then write down the username and password. You will need this information for a later step.

   You can skip this step if you plan to let FireMon use an existing account to log in.

3. Return to the FireMon GUI and add the Crossbeam device to the list of monitored devices.

   **If you are adding an X-Series device:**

   A. Select **X-Series** in the New Device window.

   B. Enter the following properties:

   **Name** as you want to see it in FireMon.

   **IP Address** of the device (required if not using DNS Name).

   **DNS Name** of the device (required if not using IP address).

   **Data Collector** that will retrieve data.

   **Licensed**: select this check box if your FireMon product license includes this device

   **User name**: the read-only login account that you created for the FireMon Data Collector

   **Password**: the password for the read-only login account that you created for the FireMon Data Collector

   **Protocol**: the communication program used between FireMon and the monitored device

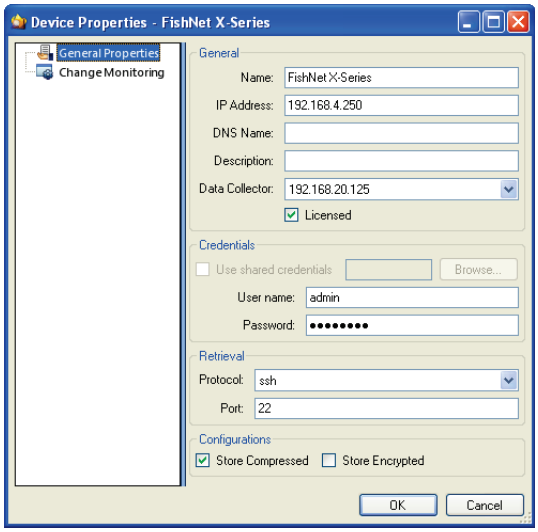
   **Port**: the device endpoint from which FireMon uses the specified protocol to retrieve device data

   C. Click **OK**.

   D. The device appears in the Devices Navigation.

   Please note that XOS device appears in the GUI as a separate device, distinct from any of the applications that run on it. For example, an XOS device running a Check Point FireWall Module will be displayed in the GUI Navigation *outside* of a Check Point CMA>FireWall Module hierarchy.

   E. Repeat this procedure for every XOS device that you want to monitor with FireMon.




X-Series Properties

**If you are adding a C-Series device:**

The C-Series OS is added as a property of the Check Point application running on it. Unlike X-Series, it is not added as a separate device.

A. Close the New Device window.

B. In the Devices Navigation of the FireMon GUI, right-click the device running on COS and select **Properties**.

C. The Properties window opens.

D. In the OS list, select **Crossbeam C-series**.

E. In the left pane of the Properties screen, click **OS**.

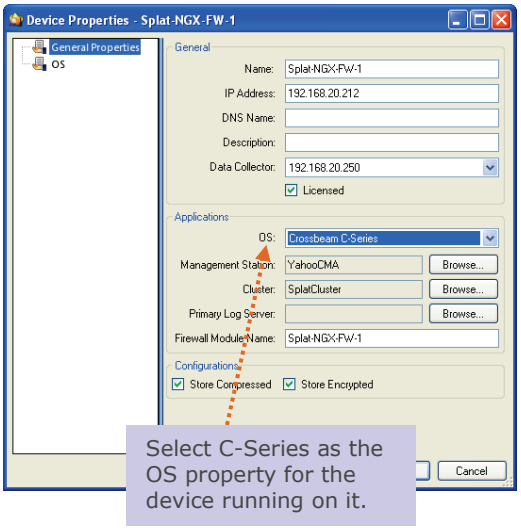
F. In the Credentials section, enter an administrator login username and password. You can use an existing account or the unique account that you created for the Data Collector.

G. In the Retrieval section, enter the port on which the device is listening and the protocol used to communicate with the Data Collector.

H. Click **OK**.

I. The COS is saved as a property for the Check Point device. It does not appear in the Devices list or Dashboards, although FireMon is monitoring it.

J. Repeat this procedure for every Check Point device running on COS.




C-Series as a Check Point Property

## Step 2: Verify Communication

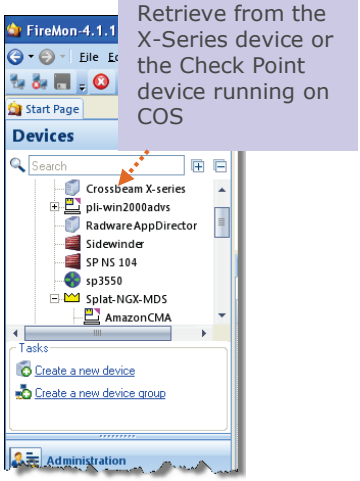
To verify that FireMon can communicate with the new device, manually retrieve a configuration.

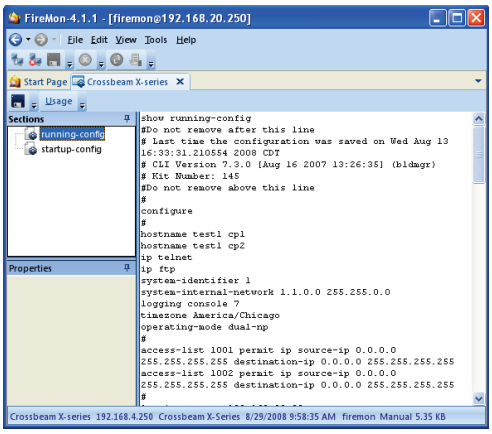
1. In the **Devices** Navigation, right-click the X-Series device that you just added and select **Retrieve Configuration**.

   If you are verifying a C-Series OS that was added as a Check Point property, right-click the Check Point device name and select **Retrieve Configuration**.

2. The Configuration Retrieval Wizard opens.
3. Click **Next**.
4. When the configuration is retrieved, a green check mark 

will appear. Click **Finish** to open the configuration.




X-Series Configuration

## Nokia

### Step 1: Configure Devices and FireMon Properties

1. Implement Syslog Notification to be sent to FireMon from your Nokia IPSO device:

   A. Navigate to the System Logging page in the Nokia Voyager window.
   B. Add the Data Collector IP address and **Apply**.
   C. Then choose a severity and **Apply**.

2. Enable SSH Server on your Nokia device.

   FireMon uses SSH to communicate to a Nokia host. The Data Collector will always attempt to use SSH v2 first and revert back to SSH v1 only if the server does not support SSH v2. FireMon supports only password-based authentication.

   To configure the SSH Server, please refer to the Nokia IPSO documentation for specific instructions appropriate for the version of IPSO running.

   A. Enable the SSH service in IPSO.
   B. Permit Admin user to log in.
   C. Allow access using password authentication. Then write down the username and password. You will need this information for a later step.

3. In the FireMon GUI, close the New Device window. IPSO is added as a property of the Check Point application running on it. It is not added in FireMon as a separate device.

4. In the Devices Navigation of the FireMon GUI, right-click the device running on IPSO and select **Properties**.

5. The Properties window opens.

6. In the OS list, select **Nokia IPSO**.

7. In the left pane of the Properties screen, click **OS**.

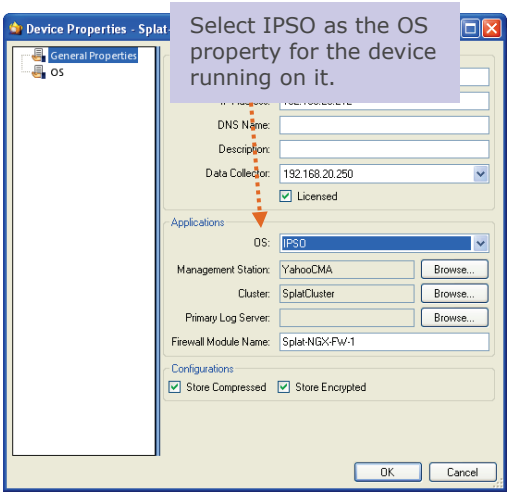
8. In the Credentials section, enter an administrator login username and password.

9. In the Retrieval section, enter the port on which the device is listening and the protocol used to communicate with the Data Collector.

10. Click **OK**.

11. IPSO is saved as a property for the Check Point device. It does not appear in the Devices list or Dashboards, although FireMon is monitoring it.

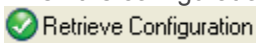
12. Repeat this procedure for every application running on IPSO.



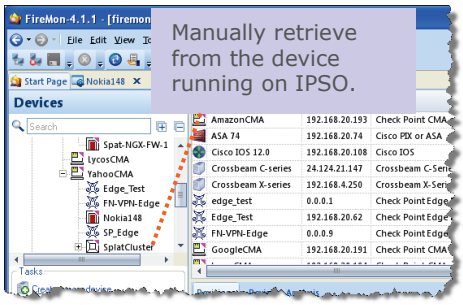

IPSO as a Check Point Property

## Step 2: Verify Communication

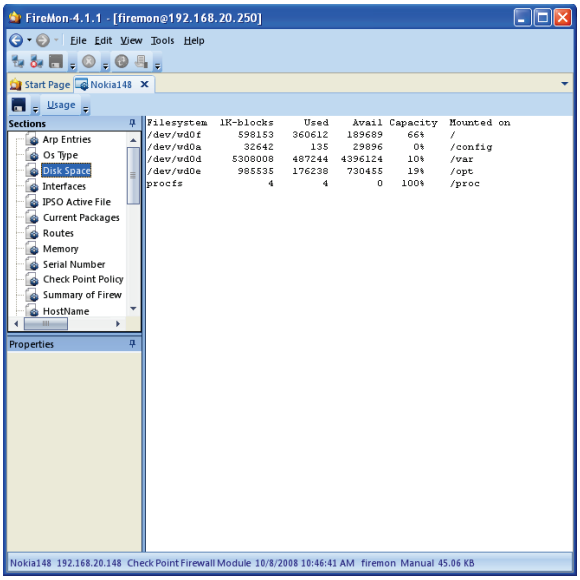
To verify that FireMon can communicate with the new device, manually retrieve a configuration.

1. In the **Devices** Navigation, right-click the device that is running on IPSO and select **Retrieve Configuration**.
2. The Configuration Retrieval Wizard opens.
3. Click **Next**.
4. When the configuration is retrieved, a green check mark 

will appear. Click **Finish** to open the configuration.




IPSO Retrieval on a Check Point Device




IPSO Configuration on a Check Point Device

## Secure Computing/McAfee

### Step 1: Configure Devices and FireMon Properties

1. On your Sidewinder device, enable Syslog Notifications in Sidewinder to be sent to FireMon:

   A. In **/etc/sidewinder/auditd.conf**, add the following line at the end:

   *syslog(local0 filters["type AUDIT_T_CFG_CHANGE"]*

   The text *local0* defines the facility name that you will enter in the next step. *Filters* is a list of filters. The filter listed above limits the logs to include only change audit events.

   B. In /etc/syslog.conf, add the following line below the example line "*.* @localhost":

   *local0.* @IPADDRESS

   Where *IPADDRESS* is the IP Address of your FireMon Data Collector.

2. On your Sidewinder device, create a read-write account for the FireMon Data Collector.

3. In the New Device window in the FireMon GUI, click **SecureFirewall (Sidewinder)** and click **OK**.

4. The Device Properties window opens.

5. Enter the following properties and click **OK**:

   **Name** as you want to see it in FireMon.

   **IP Address** of the device (required if not using DNS Name).

   **DNS Name** of the device (required if not using IP Address).

   **Data Collector** that will retrieve data.

   **Licensed**: select this check box if your FireMon product license includes this device

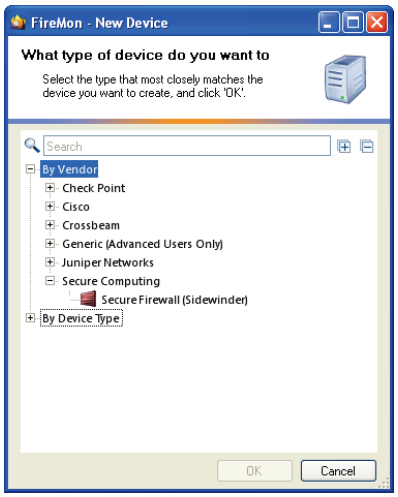
   **User name**: the read-write login account that you created for the FireMon Data Collector

   **Password**: the password for the read-write login account that you created for the FireMon Data Collector

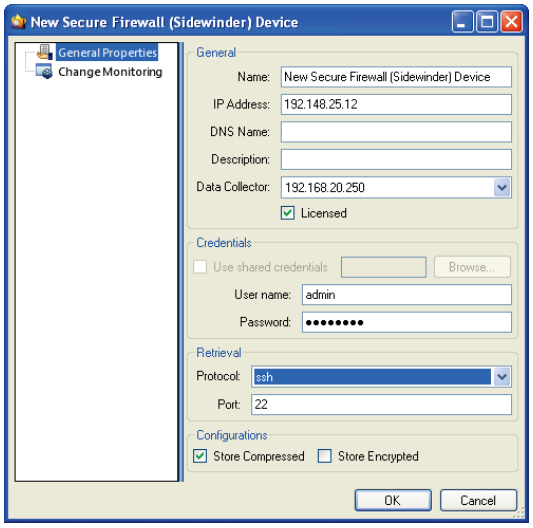
   **Protocol**: the communication program used between FireMon and the monitored device

   **Port**: the device endpoint from which FireMon uses the specified protocol to retrieve device data

6. The device appears in the **Devices** Navigation.



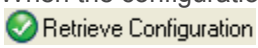

New Device Window




Sidewinder Properties

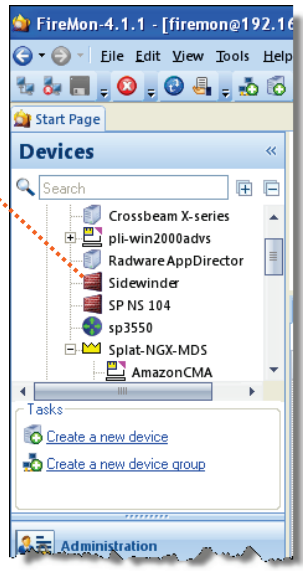
## Step 2: Verify Communication

To verify that FireMon can communicate with the new device, manually retrieve a configuration.

1. In the **Devices** Navigation under All Devices, right-click the Sidewinder device and select **Retrieve Configuration**.
2. The Configuration Retrieval Wizard opens.
3. Click **Next**.
4. When the configuration is retrieved, a green check mark 

will appear. Click **Finish** to open the configuration.

Manually retrieve from the Sidewinder device.




List of Devices

# 5 Next Steps

Now that your FireMon product is fully functional you can start exploring the primary features of FireMon.

## Explore

### Change Management

Using FireMon's configuration comparison tools, see exactly how a configuration has changed. Differences are displayed in the visual context of the configuration. Or schedule a Change Report to show incremental change detail and automatically email change analysis when a new configuration is detected. See the *User's Guide* for more information.

### Policy Usage Analysis

A short, simple rule base in your security policy is easy to manage and improves firewall efficiency. With FireMon's Usage Analysis feature, discover the statistics and data that will help you reduce policy complexity. See the *User's Guide* for more information.

### Reports

Reports are schedulable, formatted output of FireMon's configuration analysis. You determine when the report is run -- on demand or according to a schedule – and who should receive the results. Additionally, you can choose the file format that you want output to appear in. See the *User's Guide* for more information.

### Policy Test

Test a policy for connectivity through a firewall. Policy Test is just one feature in FireMon's Compliance capability, which helps you validate device configurations for compliance with corporate or governmental regulations. See the *User's Guide* for more information.

## Resources

### *Administrator's Guide*

This document is for users responsible for managing the FireMon software. It explains user permissions and management, Database backups, monitored device properties.

### *User's Guide*

This document is for users who use the day-to-day features of FireMon. It describes FireMon's change management, compliance, and policy optimization features, and explains how to use the FireMon Graphical User Interface (GUI).

### *Appliance Configuration Guide*

This document is for users managing the FireMon server components on an SPX appliance (Linux). It includes the first-time configuration wizard, and additional commands for viewing and changing the appliance configuration.

### User Center

The User Center is a Web site where Secure Passage customers with valid software subscriptions can download software updates, documentation and product licenses; and submit Support tickets. The site is located at https://usercenter.securepassage.com. A first-time login was emailed to your company along with your FireMon product license.

# A Appendix

This Appendix provides information that will help you plan your FireMon deployment. It also includes a worksheet to help you set up monitoring in FireMon.

## System Sizing Recommendations

To allocate space on your system for processing activities and data, please follow these guidelines. If you have sizing questions regarding your organization's system or questions that are not addressed below, please email our Support team at support@firemon.com.

If you are deploying FireMon on Linux, your organization has already considered these recommendations and purchased the SPX appliance that would best suit your needs.

**A. Server Operating System**:

250 megabytes (MB) of memory for other processing activities

**B. Application Server (AS) memory**:

- 1 gigabyte (GB) free for AS process execution

  These processes include running comparisons, auditing, normalization, etc.
- 50 MB for AS runtime
- 1 MB per application (inventory cache)
- 100 MB for Firebird database server

**C. Hard drive space**:

25 MB per policy saved. Use the calculation below to estimate how much space is needed on your system.

**Calculation:**

**FW** x **AvgInstalls** x **Weeks** = ***Policies***

***Policies*** x 25 = ***Recommended Space***

Where the following is true:

**FW** is the number of firewalls
**AvgInstalls** is the average number of installs per firewall per week
**Weeks** is the number of weeks of history
***Policies*** is the estimated number of policies

*Example*

300 firewalls (**FW**)

Average 1 install per week (**AvgInstalls**)

1 year of storage (**Weeks**)

300 x 1 x 52 = 15,600

15,600 x 25 = 390,000 MB

The recommended hard drive space for this example is 390,000 MB (or 390 GB).

Please note, however, that depending on the FireMon features you use, the space requirement may increase.

**D. Data Collector (DC)**:

- 150 MB for general DC operation and to handle the spikes in memory utilization during retrieval operations
- 12 MB for each Check Point management server (CMA or SmartCenter) under revision
- 1 MB / firewall logging. This allowance should be more than sufficient for a rule base of 300 rules and 3000 objects.
- Nokia and other devices or platforms that are monitored by Syslog have no special memory requirements. Allow 1 MB per application.
- The processor for log monitoring processes up to 1,200 logs per second per 3GHz processor.

## Communication Protocols

The communication protocols listed here will help you complete the Device Worksheet on the following page and Monitoring Setup.

| Port Number (Type) | Connection | Function |
|---|---|---|
| 3192 (TCP) | From GUI to AS (Required) | Allows FireMon GUI to log into the AS. |
| 3193 (TCP) | From AS to DC (Required) | The DC listens on this port for connections from the AS. The AS connects to the DC for several reasons: to inform the DC that the AS is up and running, to begin a manual retrieval, and to send updated configurations to the DC for use in usage matching. |
| 18190 (TCP) | From DC to management server | Default FireWall-1 port for CPMI communication. Used to retrieve policies from the management server. |
| 18184 (TCP) | To establish a LEA connection between DC and a Check Point management server | FireMon uses Log Export API (LEA) to connect to a Check Point log server. |
| 18210 (TCP) | Between DC and management server | Used to generate certificate used in encrypted communication between DC and Check Point management server. |
| 22 (TCP) | SSH from DC to devices that are not from Check Point | Used to retrieve configuration information. |
| 23 (TCP) | Telnet from DC to devices that are not from Check Point | Used to retrieve configuration information. |
| 25 (TCP) | From the AS to an SMTP server | Allows the FireMon AS to send email notification of change events or reports.<br>Required only if user wants to use email notification or Scheduled Reports. |
| 514 (UDP) | From the DC to a Syslog server | Required only if you are using a central Syslog for logging. |
| 80 (TCP) | From the GUI to the AS | Default HTTP port for report images hosted on the Application Server. Required if you want to host report images and styles on your Application Server. |
| 8443 (TCP) | From the DC to an NSM (required) | Default port for SSH communication. Used to retrieve policies from the NSM. |

## Device Worksheet

Use this sheet to help you gather information about the devices that you want to monitor. You will enter this information in the FireMon GUI during the monitoring setup process. See the Communication Protocols sheet for a list of ports and protocols.

| **Device Type** (*ex.* Firewall) | **Vendor** (*ex.* Cisco) | **Device Name** (as it will appear in FireMon) | **IP Address** | **Port** | **Protocol** |
|---|---|---|---|---|---|
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

# Alternate Scenarios & Troubleshooting

## Adding Devices

### Check Point – Manual Object Creation

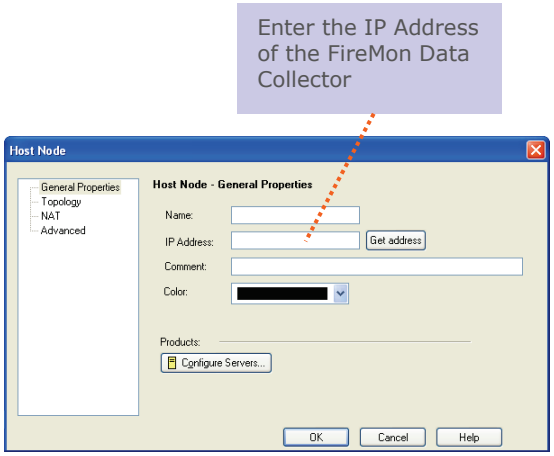
You must manually create the OPSEC application object for the FireMon Data Collector if any of the following apply:

- You cannot enable CPRA.
- You cannot provide a read/write administrator login for one-time use.
- You have already created the OPSEC application object or you plan to create it.

Complete the following steps on each CMA or SmartCenter that you want to monitor:

1. In SmartDashboard™, connect to the management server.
2. Create a new network object host node for the FireMon Data Collector:

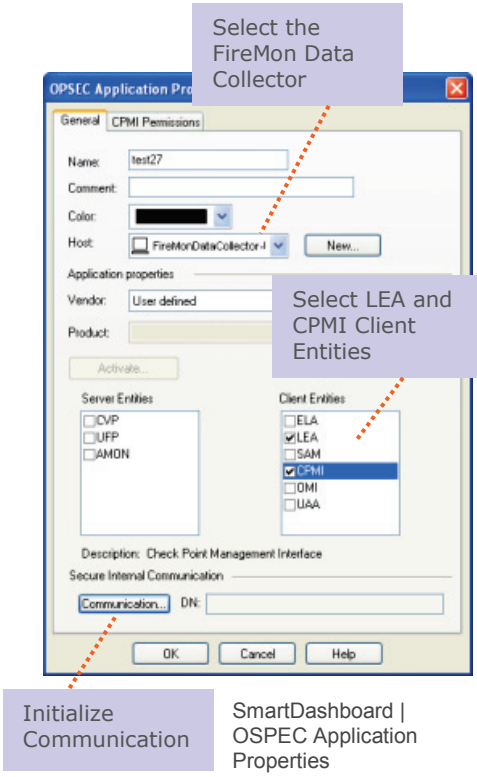
   A. In the Network Objects list, right-click **Nodes** and select **New Node>Host**.
   B. The Host Node General Properties window appears.
   C. Enter the name and the IP address of your FireMon Data Collector.
   D. Click **OK**.




SmartDashboard | New Host Node

3. Create the Data Collector OPSEC Application:

   A. In the Servers and OPSEC Applications tab, right-click **OPSEC Applications**. Then select **New>OPSEC Application**.
   B. The OPSEC Application Properties window appears.
   C. In the **Host** list, select the Data Collector Host that you created earlier.
   D. In the Client Entities box, select **LEA** and **CPMI** check boxes.
   E. Click **Communication** and enter and confirm an Activation Key. Then write down the Activation Key that you entered. You will need it later when you create your devices in FireMon.
   F. Click **Initialize**. The Trust state should be “Initialized but trust not established.” This status will change once FireMon establishes communication with the log server.
   G. **Close** and **Save** the OPSEC application object.



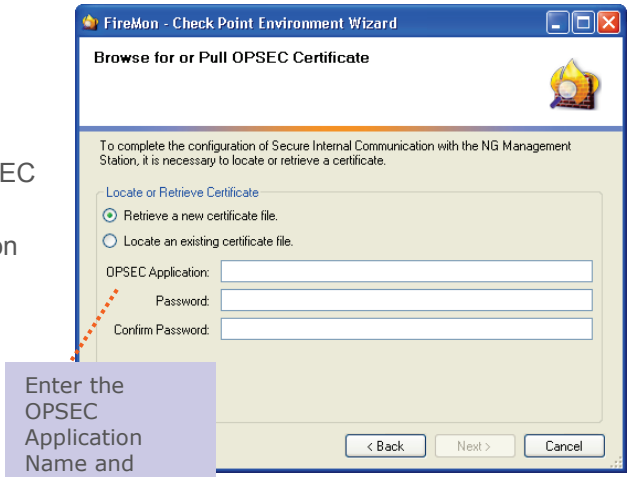

SmartDashboard | OSPEC Application Properties

4. Ensure that all users with read/write access are logged out of SmartDashboard.

5. Return to the Check Point Environment Wizard in the FireMon GUI. The “Browse for or Pull OPSEC Certificate” screen should be open.

6. Select **Retrieve a new certificate file** and enter the OPSEC Application Name and Activation Key. Then click **Next**.

7. Continue to step 17 in the “Configure Devices and FireMon Properties” for Check Point.




FireMon Check Point Environment Wizard

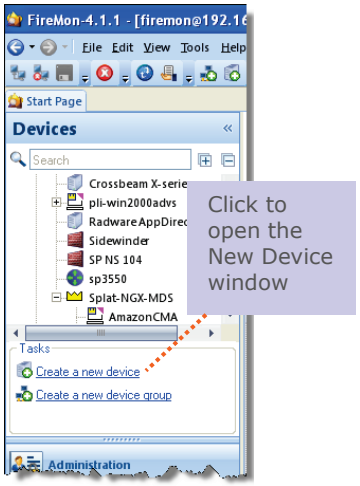
**About the OPSEC Application**
OPSEC is Check Point’s Open Platform for Security, which allows third-party applications like FireMon to plug into the OPSEC framework via published APIs like LEA and CPMI.

The FireMon Data Collector uses the Check Point Management Interface (CPMI) to communicate with Check Point management servers and Log Export API (LEA) to communicate with log servers. Communication is authenticated and encrypted using Secure Internal Communication (SIC).

To use SIC, an OPSEC application object representing the Data Collector must be created in the CMA or SmartCenter database and the resulting certificate retrieved.

## I Can’t Find the New Device Window

You can open the New Device window by clicking the **Create a New Device** text link in the Devices Navigation.




Devices Navigation

## I Did Not Set Up Monitoring After the First Run Wizard

When you are ready to set up monitoring, complete the following steps:

1. Open the FireMon GUI and connect to your Application Server.
2. In the Navigation, click **Devices**.
3. Click the **Create a New Device** text link.
4. The New Device Window opens.
5. Continue to Step 2: Add Devices (page 15) in this document.

## Configuration Retrieval Fails

If you received an error after attempting to manually retrieve a configuration, complete the following steps.

1. Verify that you have completed all of the steps in Set Up Monitoring.
2. Verify that the username and password in the device properties in FireMon are correct. To view the device properties, right-click the device name in the Devices Navigation and select **Properties**.
3. Manually retrieve a configuration by right-clicking the device name in the Devices Navigation and selecting **Retrieve Configuration**. Make sure that you select the **Include debug output** check box.
4. If manual retrieval fails, copy the debug output and paste it into an email message. Send the message to support at support@firemon.com.