

SOPHOS

Security made simple.



Sophos Firewall Manager Web Interface Reference and Admin Guide v1605

For Sophos Customers

Document Date: June 2017

Contents

| | |
|--|-----------|
| Introduction..... | 4 |
| Using Admin Console..... | 5 |
| Supported Browsers..... | 6 |
| Navigating through the Admin Console..... | 6 |
| Menus..... | 7 |
| Tool Tips..... | 9 |
| Notification pop-ups..... | 9 |
| Common Operations..... | 9 |
| Set Schedule..... | 9 |
| Synchronize..... | 10 |
| Entity Usage Reference..... | 10 |
| Editing an Entity..... | 10 |
| Deleting an Entity..... | 11 |
| Sorting Lists..... | 11 |
| Filtering Lists..... | 11 |
| Configuring Column Settings..... | 11 |
| Reordering Lists..... | 11 |
| Summary..... | 11 |
| Templates..... | 12 |
| System & Monitor..... | 12 |
| Device Settings..... | 12 |
| Managed Devices..... | 12 |
| Maintenance..... | 26 |
| Firmware..... | 29 |
| Scheduled Task..... | 30 |
| Dynamic Objects..... | 30 |
| Change Control..... | 35 |
| Monitor..... | 40 |
| Device Monitor..... | 40 |
| Graphs..... | 42 |
| Alerts..... | 44 |
| Event Viewer..... | 47 |
| System Settings..... | 49 |
| Administration..... | 49 |
| System..... | 61 |
| Network..... | 73 |
| Maintenance..... | 77 |
| Content Distribution..... | 80 |
| Diagnostics..... | 81 |
| Appendix A - Compatibility with SFOS..... | 83 |

Copyright Notice..... 84

Introduction

Sophos Firewall Manager (SFM) provides comprehensive central management of Sophos Firewalls to Enterprises and MSSPs. With a range of features, SFM simplifies security management for actions like rapid deployment of organization-wide security policies and updates for better protection of dispersed networks, offering benefits of reduced cost, complexity and time. Sophos Firewall Manager (SFM) is available in hardware, software and virtual form-factors to suit any environment.

The Sophos Firewall Manager UI offers you 3 work areas: Device Configuration, Template Configuration, and System Management.

Device Configuration

The Device Configuration work area allows you to manage policies and configurations of individual or group of Sophos Firewall devices. You can select an individual device or device group and use menu items in the left panel to edit Policies, Settings and Objects like in your Firewall UI.

Template Configuration

The Template Configuration work area allows you to create re-usable configuration templates allowing you to set up a new firewall at branch or customer office in minimum time. You have an option to add a template using an existing device configuration, clone an existing template, or setup a fresh template. You can edit the template configuration by using menu items in the left panel to edit Policies, Settings and Objects like in your Firewall UI. Once ready, you can provision the template to one or more firewall devices as per your need.

System Management

The System Management work area lets you manage device settings, monitoring settings and your SFM system settings.

- Device settings: You can add or remove managed devices or device groups, add or remove templates, upgrade firmware of managed devices, create and manage dynamic objects, and change control and logging.
- Monitoring settings: You can edit monitoring settings, setup email alerts, view device events and logs, view management system events, and integrate with Sophos iView V2.
- System settings: You can manage SFM users, and set up role-based access, SFM API, Network Settings, Diagnostics, and more.

Dashboards & Monitoring

Sophos Firewall Manager offers multiple dashboards for a quick snapshot and easy monitoring of your managed firewalls.

- Device Monitor
 - Flat view and card view allow you to monitor the status (Critical, Warning, Normal) of managed devices across a set of parameters for Security, Resource, License and Availability, based on their threshold values.
 - In flat view, devices that need attention are automatically listed at the top on the basis of their monitor status.
 - You have the flexibility to customize threshold values for Critical, Warning and Normal levels as per your needs.
- Home and Group-level Dashboard
 - Device Info: Summary of managed devices like the count of managed devices, unsynchronized devices, and disconnected devices.
 - Device monitor summary: A snapshot of firewall count that requires attention in terms of Security, Resource, License, Availability.
 - A list of managed firewalls by their model number, and more.

Group-level dashboard lets you filter the above view for a device group.

- Device Dashboard - It offers you insights into security, resource, license and availability parameters along with device and connection information to enable you to take necessary action
- Alert - Configure alert profiles for one or more firewalls or Firewall group to get alert notifications over email. This includes alert notifications for parameters like subscription expiry, Device disconnected from central management, Device Gateway status change, VPN connection status change, along with counts of Intrusion attack, ATP events exceed, Web virus, Objectionable + Unproductive surfing hits, and percentage of endpoints with Red health exceeding a threshold limit.

Using Admin Console

Sophos Firewall Manager uses a Web 2.0 based easy-to-use graphical interface termed as Admin Console to configure and manage the device.

You can access the device for HTTP and HTTPS web browser-based administration from any of the interfaces. Device when connected and powered up for the first time, it will have a following default Admin Console Access configuration for HTTP and HTTPS services.

| Services | Interface/Zones | Default Port |
|----------|-----------------|---------------|
| HTTP | LAN, WAN | TCP Port 80 |
| HTTPS | WAN | TCP Port 4444 |

The administrator can update the default ports for HTTP and HTTPS services from **System Management > System Settings > Administration > Settings**

Admin Console Language

The Admin Console supports multiple languages, but by default appears in English. Apart from English, Brazilian-Portuguese, Chinese-Simplified, Chinese-Traditional, French, German, Italian, Japanese, Korean, Russian and Spanish languages are also supported. Administrator can choose the preferred language at the time of logging in.

Administrator can also specify description for various policies, services and custom categories in any of the supported languages.

Log on procedure

The log on procedure authenticates the user and creates a session with the Device until the user logs-off.

To get the login window, open the browser and type LAN IP Address of the device in browser's URL box. A dialog box appears prompting you to enter username and password.

Below are the screen elements with their description:

Username

Enter user login name.

If you are logging on for the first time after installation, use the default username.

Password

Specify user account password.

Dots are the placeholders in the password field.

If you are logging on for the first time after installation with the default username, use the default password.

Log on to

To administer device, select **Admin Console**.

Login button

Click to log on the Admin Console.

Home appears as soon as you log on to the Admin Console which provides a quick and fast overview of all the important parameters of your added devices and SFM System.

Log out procedure

To avoid un-authorized users from accessing Sophos Firewall Manager, log off after you have finished working. This will end the session and exit from device.

Supported Browsers

You can connect to Admin Console of the device using HTTP or a secure HTTPS connection from any management computer using one of the following web browsers:

Latest version of Firefox (recommended), latest version of Chrome, latest version of Safari, or Microsoft Internet Explorer 9 onwards. JavaScript must be enabled.

The minimum screen resolution for the management computer is 1280 X 768.

Navigating through the Admin Console

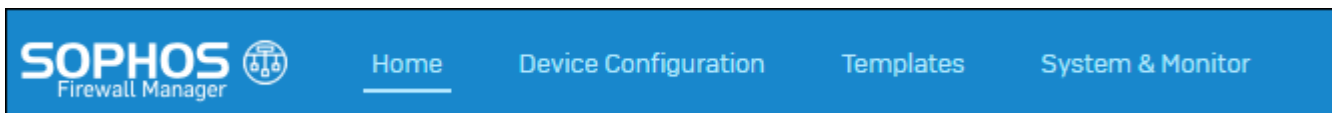
The three parts of the admin Console:

- Area Selector
- Navigation Bar
- Content Pane
- Button bar

Use the menus, lists, and configuration pages to configure most settings. Configuration made through Admin Console take effect after some time as it takes time to copy the entire configuration on to the device.

Work Area Selector

The Sophos Firewall Manager UI offers you three work areas: Device Configuration, Template Configuration, and System Management. To select any work area, select the icon on the top right corner of the Home.



Once an area is selected, the Navigation bar changes based on the selected work area.

Device Configuration allows you to navigate through pages through which you can manage Device Groups or individual devices. The navigation bar changes dynamically for Device Group and individual device. You can select device group or any device **Device Groups** or **Device** on the Dashboard top panel.

Navigation Bar

The navigation bar on the leftmost side provides access to various configuration pages. Menu consists of sub-menus and tabs. On clicking menu item in the navigation bar, related management functions are displayed as submenu items. On clicking submenu item, all the associated tabs are displayed. To view page associated with the tab, click the required tab.

The Main menu tree expands and contracts dynamically when clicked on without navigating to a submenu. When you click on a top-level heading, it automatically expands that heading and contracts the heading for the page you are currently on, but it does not navigate away from the current page. To navigate to a new page, first click on the


heading, and then click on the submenu you want navigate to. A breadcrumb on the top of the Content Pane displays the entire navigation path.









Content Pane

The center part of the page is Content Pane that changes according to the menu item and tab. Information of the menu is displayed in the content pane, which includes list of managed devices and configuration screens.

Button Bar



The Button bar on the upper rightmost corner of the every page provides access to several commonly used functions like:

- Device Search – Specify a search string and click  to search device(s) in SFM. Device(s) can be searched on following criteria:

| | |
|---|---------------|
|  | Device Name |
|  | Model |
|  | Serial Number |
|  | Firmware |
|  | Company |
|  | City |
|  | State |
|  | Country |

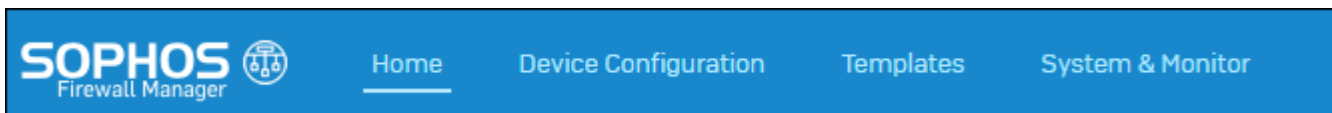
By default it yields results based on Device Name. Results display following information in tabular form: Device name, Serial number, Company name, Status and Firmware.

Click Device Name to go the dashboard of that device.

- Alerts – Click to view list of alerts generated by SFM.
- Discovery – Click to view list of devices sending heartbeat packet to the SFM. Click  icon to add newly discovered devices using Add Device Wizard or  icon to delete the device.
- Errors – Displays total number of generated errors.
- Monitor - Click to view the Device Monitor graphs which displays critical health status of the managed devices.
- Help – SFM includes a Web-based help online help, which can be viewed from any of the page of admin console. Click **Help** to open the context-sensitive help for the page.
- Language - Click to change device language.
- More - Click to view more options.
 - Wizard – Click to run Network Configuration wizard which will guide you step-by-step through configuration of the network parameters like IP address, subnet mask and default gateway for your device.
 - Console – Click to get immediate access to CLI by initiating a telnet connection with CLI without closing admin console.
 - Support – Click to open the customer login page for creating a Technical Support Ticket. It is fast, easy and puts your case right into the Technical Support queue.
 - About Product – Click icon to open the License page.
 - Reboot Device – Click to reboot the device.
 - Shutdown Device – Click to shut down the device.
 - Logout – Click to log out from the Admin Console.

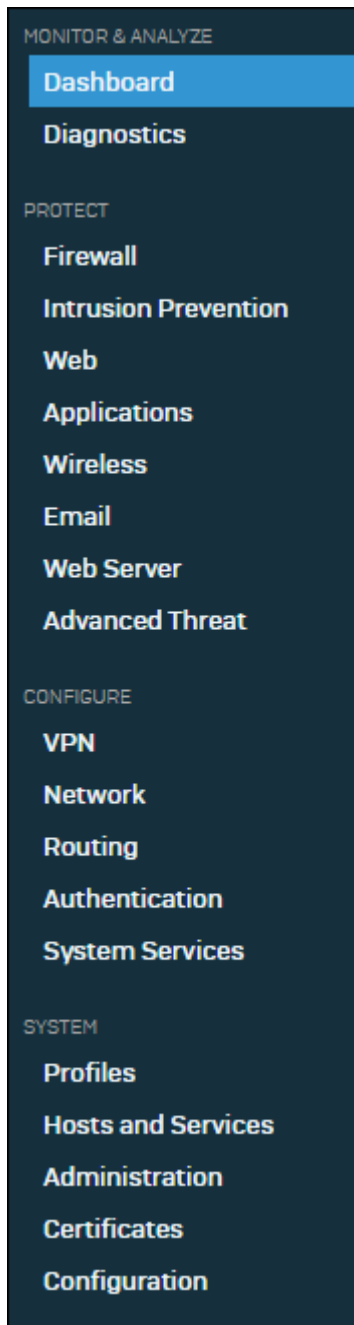
Menus

The Sophos Firewall Manager UI offers you three work areas: Device Configuration, Templates, and System & Monitor. Select any work area from the top, beside Home.




Once an area is selected, the Navigation bar changes based on the selected work area.


The navigation bar on the leftmost side provides access to various configuration pages. Menu consists of sub-menus and tabs. On clicking menu item in the navigation bar, related management functions are displayed as submenu items. On clicking submenu item, all the associated tabs are displayed. To view page associated with the tab, click the required tab.

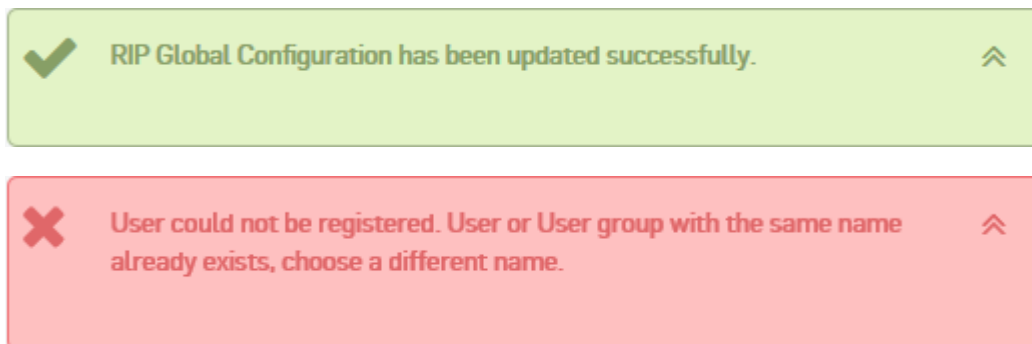


Tool Tips

To view the additional configuration information, use tool tip. Tool tip is provided for many configurable fields. Move the pointer over the icon  to view the brief configuration summary.

Notification pop-ups

A notification pop-up will be displayed at the top of the every page for error messages or action status. You can click the icon  to close the pop-up.



Common Operations

Adding an Entity

You can add a new entity like policy, group, user, rule, or host by clicking the **Add** button available on most of the configuration pages. Clicking the Add button either opens a new page or pop-up window.

You can add new items for a entity by clicking the **Add New Item**. Select items by clicking the check box and apply to add the selected items. You can also update/delete the items added.

Set Schedule

For the entire group and subgroup level configuration, administrator can update configuration immediately or schedule the update. Whenever any configuration task – add, update and delete, is done, Set Schedule page with following parameters is opened:

Synchronize Configuration - Select the time and date to update the configuration.

Immediately – Changes will be applied immediately to the device(s). However it takes some time to reflect the changes locally.

At: –Specify date and time in the format YYYY –MM-DD Hours:Minutes or select date and time from the given calendar. Configuration will be updated at the scheduled time. All the scheduled tasks are listed at **System Settings > Device Settings > Scheduled Task** page. If required, scheduled task can also be deleted from Scheduled Tasks page.

Device Time Zone – Select to apply changes as per the device time zone.

Override configuration - Select **Yes** to override existing configuration of device else select **No**.

Select Device(s) - Select **Device(s)** or **Device Group(s)** for which this task is to be scheduled.

Filter Devices - Click to filter devices on the basis of given criteria.

Select Criteria and specify the value to be matched.

- Model : Specify model.

- Firmware: Specify firmware.
- Company: Specify company name.
- Country: Specify country name.
- State : Specify state name.
- City: Specify city name.
- Device Name: Specify device name.


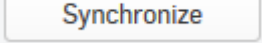


Note:

- **Filter Devices** is available only if **Device** is selected in **Select Device(s)**.
- Sophos Firewall device(s) below SFOS 16.0.0 will not be displayed for selection.


Synchronize

You can synchronize configuration of selected entities of managed device(s) with the configuration available in SFM.

To Synchronize settings, click  icon or the  button.

Entity Usage Reference

Entity Usage Reference points out the co-dependency of an entity with another entity. Entity Usage Reference lists all the dependent entities related to a particular entity. The list includes the entity, sub-entity and the device group details. Entity Usage Reference is an essential feature for the administrator so that they can identify all co-dependent entities before deleting any particular entity. If the dependency exists, the administrator must remove the dependency before deleting the entity.

To determine the Entity Usage Reference, click  . This will display the following information for the selected entity and its dependent entity(ies).

Details of selected entity

Entity

Displays the selected entity type.

Sub Entity

Displays the selected Sub Entity type.

Entity Name

Displays the name of the selected entity.

Details of dependent entities

Sub Entity

Displays the selected Sub Entity type.

Entity Name

Displays the name of the dependent entity.


Device Group

Displays the name of the device group of which the dependent entry is a part of.


Device Group Path


Display the path of the device group based on the device criteria adopted for the group.

Editing an Entity

All the editable entities are hyperlinked. You can edit any entity by clicking either the hyperlink or the  icon under the **Manage** column.

Deleting an Entity



You can delete an entity by selecting the check box and clicking the **Delete** button or  icon.

To delete multiple entities, select  individual entity and click the Delete button.

To delete all the entities, select the check box  in the heading column and click the Delete button.



Sorting Lists

To organize the list spread over multiple pages, sort the list in ascending or descending order of a column attribute. You can sort a list by clicking a column heading.

- Ascending Order icon  in a column heading indicates that the list is sorted in ascending order of the column attribute.
- Descending Order icon  in a column heading indicates that the list is sorted in descending order of the column attribute.

Filtering Lists

To search specific information within the long list spread over multiple pages, filter the lists. Filtering criteria vary depending on a column data and can be a number or an IP address or part of an address, or any text string combination.

To create filter, click the Filter  icon in a column heading. When a filter is applied to a column, the Filter icon changes to .

Configuring Column Settings

By default on every page all columnar information is displayed but on certain pages where a large number of columnar information is available, all the columns cannot be displayed. It is also possible that some content may not be of use to everyone. Using column settings, you can configure to display only those numbers of columns which are important to you.

To configure column settings, click **Select Columns** and select the check box against the columns you want to display and clear the check box against the columns which you do not want to display. All the default columns are grayed and not selectable.

Reordering Lists

You can reorder the Security Policies/Groups by dragging and dropping. On successful reordering, a status message will be displayed. Following can also be reordered:

- IPS Policy Rules
- Application Filter Policy Rules

Summary

For convenience in reviewing the firewall rule, a summary of the firewall rule is auto-populated along-side the configuration windows. In addition to this, you can click any summary element to scroll up or down, directly to the configuration section.

Templates

Template is a customizable set of policy configuration including commonly used objects, services and other configurations. SFM allows the administrator to define templates for storing global configurations. The configuration stored in a template can be directly applied to any managed Device(s) or Device group(s).

Template enables ease-of-administration by eliminating the need of configuring same entities on the Devices individually. Policy configuration using templates reduces administrative efforts in large enterprises and MSP networks where new Devices are added frequently.



Note: All policy configuration entities for Device Group level can be added to a template, except the following entities, which are outside the scope of templates:

- Administrator Password
- Synchronize

System & Monitor

System Management menu is meant to manage and configure the basic system options for the Firewall Manager. This includes the basic network settings to connect the Firewall Manager to the corporate network, the configuration of administrators and their access privileges, managing and updating firmware for the Firewall Manager, as well as managed Devices.

System allows you to configure the following settings:

- [Device Settings](#)
- [Monitoring](#)
- [System Settings](#)

Device Settings

Device Settings menu enables the administrator to add devices to the Firewall Manager. Once the devices are added, they can be organized into groups based on various criteria. The administrator can manage and configure devices or groups from Device Management menu. The administrator can also add dynamic objects for all managed devices. The menu also allows administrator to take and download backup of managed devices and restore it later on. Additionally, it gives visibility and control over scheduled tasks and Change Control events for managed devices.

Device Settings lets you configure the following settings:

- [Managed Devices](#)
- [Maintenance](#)
- [Firmware](#)
- [Schedule Tasks](#)
- [Dynamic Objects](#)
- [Change Control](#)

Managed Devices

Use the Managed Devices menu to add and manage devices using the Firewall Manager.

Managed Devices menu allows you to configure the following settings:

- [Devices](#)

- [Device Discovery](#)
- [Device Group](#)
- [Template](#)

Devices

Use the Devices page to add, edit, delete and reboot devices from the Firewall Manager.

To add or edit device details, go to **System Management > Device Settings > Managed Devices > Device Configuration**

You can configure the following Device Settings:

- [Add/Edit](#)
- Reboot – Click the reboot icon in the Manage column against the device to be rebooted. The device can be rebooted immediately or scheduled at a later time.
- More
 1. [Add Device Wizard](#)
 2. [Export Device List](#)
 3. [Export Device IP Change Report](#)

Add Device

Use the Add Device page to add new devices or edit device details.

1. Go to **System Management > Device Settings > Managed Devices > Device Configuration** and click **Add**.
2. Specify Device details based on the given description.

Device Name

Specify device name, which uniquely identifies the Device.

Description

Specify description for the device.

Serial Number

Specify the device serial number.

IP/Domain

Specify IP address assigned to the WAN Interface of the device.

Admin Username

Specify Administrator Username of the device.

Password and Confirm Password

Specify Administrator Password of the device.

Communication Mode

Specify communication mode to manage the device from Firewall Manager.

Available options: **Central Management will push updates to this Device:**

Select if the managed device is directly accessible from Firewall Manager i.e. there is no intermediate NAT box. Specify **Access Protocol** and **Access Port** number to communicate with managed device.

This Device will fetch updates from Central Management:

Select if the managed device is behind NAT box e.g. ADSL. In that case the device will first poll Firewall Manager in interval of 1 (one) minute for any configuration updates available. If the updates are available the managed device will pull those updated configuration settings.

Enable Change Control (CCL)

Enabling Change Control allows the administrator to maintain list of configuration revisions. Configuration Revisions are the configuration changes synchronized by the Firewall Manager.

The administrator can update the CCL settings from **System Management > Device Settings > Change Control** page.

Template

Select configuration template which has to be applied on the device.

Users

Add Firewall Manager's Administrator who can manage the device.

Administrator Information

Click hyperlink to add additional information of administrator.

Administrator Name

Specify name of the Administrator.

Contact Number

Specify contact number of the Administrator.

Email ID

Specify email ID of the Administrator.

Test Connection

Click to test the connectivity between Firewall manager and the managed device.

Device Name *

Description

Serial Number *

Host Name *

IP/Domain *

Admin Username *

Password *

Communication Mode *

Access Protocol * HTTPS

Access Port * 4444

Template

User

Add New Item

(Admin user has access to all the devices irrespective of above selection.)

[Administrator Information](#)

Figure 1: Add Device

3. Click Save.

Add Device Wizard

The Add Device Wizard takes you step-by-step through process of Device addition and configuration of certain core features of Device management like firmware, backup & restore and template configuration.

Wizard is divided into six sections:

1. Device
2. Communication
3. Firmwares
4. Backup
5. Template
6. Summary

1. Go to **System Management > Device Settings > Managed Devices > Device Configuration** and select **More > Add Device Wizard**.

You can also run Add Device Wizard from Device Discovery notification.

2. Add Device Details.

- a) Specify Device name, which uniquely identifies the Device.
- b) Specify Device Key. If you are running the wizard from Device Discovery notification then this field will reflect Device key automatically.
- c) Specify IP address assigned to the WAN Interface of the Device.
- d) Specify Administrator Username of the Device.
- e) Password for the above mentioned Administrator Username of the Device.
- f) Specify description if required.
- g) Click to enable Enable Change Control (CCL).
- h) Click hyperlink to add additional information of Firewall Manager Administrator.
- i) Specify name of the Administrator.
- j) Specify contact number of the Administrator.
- k) Specify email ID of the Administrator
- l) Click **Next** to go to Communication Mode details or **Done** to complete the wizard.

Provide the following information of the Sophos Device:

Device Name *


Serial Number *

IP/Domain *

Admin Username *

Password *

Description

Enable Change Control (CCL) 

[Administrator Information](#)

Figure 2: Device Information

3. Configure Communication Mode Details.

- a) Specify device communication mode to manage the device from Firewall Manager.

Central Management will push updates to this device

Select if the managed device is directly accessible from Firewall Manager i.e. there is no intermediate NAT box. Specify access protocol and port number to communicate with the managed device.

This device will fetch updates from Central Management

Select if the managed device is behind NAT box e.g. ADSL. In that case Managed device will first poll Firewall Manager device in interval of 1 (one) minute for any configuration updates available. If the updates are available the managed device will pull those updated configuration settings.

- b) Specify Protocol that is to be used to access the device for pushing configuration and synchronizing i.e. Protocol used to communicate with the device.
- c) Specify Port through which device and Firewall Manager should communicate.
- d) Specify Firewall Manager Administrator who can manage the device.
- e) Click **Back** to go to Add device Details or **Next** to go to Firmware Management or **Done** to complete the wizard

Specify how to synchronize configuration between SFM and Sophos Firewall Device:

Communication Mode * Central Management will push configuration to this Device i

Access Protocol * HTTPS

Access Port * [Test Connection](#)

This Device will fetch configuration from Central Management

User

[Admin user has access to all the devices irrespective of above selection.]

Figure 3: Define Communication Mode

4. Configure Firmware settings.

Displays current firmware version of managed and availability of latest firmware version.

- a) If the device model is already added in Firewall Manager the latest version will be displayed automatically else click **Check for Upgrades** to check availability of latest firmware version.
- b) To upgrade the device with latest available firmware click **Yes** against **Do you want to upgrade the device.** By default it is disabled.
- c) Click **Back** to go to Communication Details and **Next** to go to Backup Management or **Done** to complete the wizard

Specify if you want to upgrade Device firmware to the latest available firmware:

| | |
|------------------------------------|---|
| Current Device Firmware | N/A |
| Latest Applicable Firmware | No Upgrade available |
| Do you want to upgrade the device? | <input type="radio"/> Yes <input checked="" type="radio"/> No |

Figure 4: Upgrade Device Firmware

5. Configure Backup Management.

- a) Click **Yes** against **Do you want to restore any existing configuration backup in new device?** to restore backup of any existing device in device to be added. By default it is disabled.
- b) Select an existing device and backup to restore it in device to be added else browse the backup file from your machine and restore it in device to be added.

- c) Click **Back** to go to Firmware Management or **Next** to go to Template Management or **Done** to complete the wizard

Do you want to restore existing configuration backup in the new device?

Yes No

Use backup of other device

Select Device Devices ▾

Select Backup Select Backup ▾

Upload Backup

Choose File No file chosen

Figure 5: Restore Existing Configuration Backup

6. Configure Template Management.
- a) Click **Yes** against **Do you want to apply any configured template to the device?** to add an device with existing configuration template. By default it is disabled.
 - b) Select template to be applied.
 - c) Click **Next** to view Summary of Add Device wizard or **Back** to go to Backup Management. Click **Done** to complete the wizard

A Template is a repository to store commonly used objects, services, and configurations. It allows using same set of configuration across multiple devices. Instead of configuring the device, you can choose a template to configure the device.

Do you want to apply any existing template to the device?

Yes No

Template Template ▾

Figure 6: Select Template to Configure Device

7. Review configuration summary.
- Summary page displays summary of the added device which includes Device Name, Device Key, IP/Domain, Admin Username, Communication Mode, Access Protocol, Access Port, Firmware Upgrade status, Restore Backup status, Template application status.
- Click **Finish** to complete the wizard or **Back** to go to Template Management.

| | |
|------------------------------|---|
| Device Name | SF1 |
| Serial Number | 3201 |
| IP/Domain | 10.10.10.10 |
| Admin Username | Admin |
| CCL | Disabled |
| Communication Mode | Central Management will push configuration to this Device |
| Access Protocol | HTTPS |
| Access Port | 4444 |
| Upgrade Firmware | No |
| Restore Backup | No |
| Apply configuration template | No |

Figure 7: Summary

Export Device List


Export Device List option is used to export the list of all managed devices added in the Firewall Manager.

The list is exported in excel format containing the following details for each device which includes Device Name, Device Key, IP/Domain, Connection Status, Firmware Version, IPS Version, AV Version, Webcat Version, License Subscription Expiration, Last backup Time, Upstream Bytes and Downstream Bytes.

Device List report is generated automatically at 11:50 PM Daily by default and the previous report is overwritten by the new report. To see the last generated report, go to **System Management > Device Settings > Managed Devices > Device Configuration** and select **More> Export > Device List**

To generate and download the report manually, follow the steps shown below.

1. Go to **System Management > Device Settings > Managed Devices > Device Configuration** and select **More> Export > Device List**.
2. Click **Generate** to generate the report.
3. You should see the **Download** hyperlink for the generated report. Click the hyperlink to download the report.

 **Note:** The manually generated report will overwrite the previously generated report.

Export Device IP Change Report


Export Device IP Change Report option is used to export the IP Address revisions for each added device.

Device IP Change Report displays IP address changes or revisions for last 30 days.

This report is generated automatically 11:50 PM Daily.

To download the report, follow the steps shown below.

1. Go to **System Management > Device Settings > Managed Devices > Device Configuration** and select **More> Export > Device IP Change Report**.
2. Click **Download** to download the report in Excel file format.

 **Note:**
The report is exported in the excel format which includes IP change information based on Device Name, Device Key, Time, Old IP and New IP.

Device Discovery

Use the Device Discovery page to view the devices which are sending heartbeat packet to the Firewall Manager. This page allows you to add these Devices to SFM.

You can View, Add or Delete the discovered devices. Adding discovered devices is similar to [adding new devices](#).

Device Groups

Device Groups are logical grouping of managed devices for ease of administration.

Administrator may want to divide the managed devices into groups for the following reasons:

- Configure group-shared settings and then update the configurations on the devices at once. For example, group all the devices that need to upgrade subscription and upgrade all the devices simultaneously.
- Manage a great number of devices more efficiently.
- Group the devices according to their locations (country/state/city), ownership/company/departments, firmware, device name and device models.



Note: Single device can be part of different groups.

Using Device Groups page, you can:

- [Add/Edit device groups](#)
- Delete existing device groups

Add Device Groups

1. Go to **System Management > Device Settings > Managed Devices > Device Groups**. Click **Add** to create a new group or Edit Icon to modify the details of the group.
2. Specify group name, which uniquely identifies group.
3. Specify Devices to be grouped based on the available options.

Model

Firmware

Company

Country

State

City

Device Name: Specify group condition criterion.

Available options: Starts with, Contains, Substring, Ends with.

| | |
|-----------------------|-------------------------------------|
| Device Group Name * | <input type="text"/> |
| Device Group Criteria | 1 <input type="text" value="None"/> |
| | 2 <input type="text" value="None"/> |
| | 3 <input type="text" value="None"/> |

Figure 8: Add Device Group



Note: You can select Device Name as a criterion multiple times. All the Devices starting with specified name prefix will be grouped dynamically.

4. Click **Save**.

Templates

Template is a customizable set of policy configuration including commonly used objects, services and other configurations. SFM allows the administrator to define templates for storing global configurations. The configuration stored in a template can be directly applied to any managed Device(s) or Device group(s).

Template enables ease-of-administration by eliminating the need of configuring same entities on the Devices individually. Policy configuration using templates reduces administrative efforts in large enterprises and MSP networks where new Devices are added frequently.



Note: All policy configuration entities for Device Group level can be added to a template, except the following entities, which are outside the scope of templates:

- Administrator Password
- Synchronize

Template Dashboard

Template dashboard displays summary of the selected template along with the recent activity log. To view the details of individual template, go to **Template Configuration** and select a template. This page displays following information for selected template:

- Template Summary
- Recent Activities

Template Summary

Displays the name of configuration entity along with number of entries for each entity.

Policies

Displays the name of **Policies** configured along with number of entries.

Protection

Wireless Protection

Displays name of the **Wireless Protection** configurations along with number of entries:

- Wireless Networks
- Mesh Networks
- Access Point Groups
- Hotspots
- Hotspot Voucher Definition
- Rogue AP Scan

Web Protection

Displays name of the **Web Protection** configurations along with number of entries:

- Web Proxy
- Web Content Filter > Configurations
- Web Filter Policies
- Custom Web Category
- URL Group
- Surfing Quota
- File Type
- Malware Protection

Application Protection

Displays name of the **Application Protection** configurations along with number of entries:

- Application Filter
- Traffic Shaping Settings

Web Server Protection

Displays name of the **Web Server Protection** configurations along with number of entries:

- Web Servers
- Web App Protection Policies
- Web App Authentication Policies
- Web App Auth Templates
- Certificate
- Certificate Authority
- Certificate Revocation Lists

Email Protection

Displays name of the **Email Protection** configurations along with number of entries:

- Email Configuration
- Scanning Rules > SMTP/S Malware Scanning Rules
- Scanning Rules > POP3/S and IMAP/S Malware Scanning Rules
- Scanning Rules > Content Scanning Rules
- SPX Configuration
- SPX Templates
- Data Protection
- Address Group
- Email Archiver
- Quarantine Digest Settings
- Trusted Domain
- Malware Protection

System Networks

Displays name of the **Network** configurations along with number of entries:

- Wireless Networks
- Mesh Networks
- DNS > DNS Configuration
- DNS > DNS Host Entry
- DNS > Request Routing
- DHCP Relay

Routing

Displays name of the **Routing** configurations along with number of entries:

- Upstream Proxy
- Static Route

VPN

Displays name of the **VPN** configurations along with number of entries:

- IPsec
- L2TP Settings
- L2TP Connections
- PPTP

- SSL VPN Settings
- SSL VPN (Site to Site) > Server Connection
- SSL VPN (Site to Site) > Client Connection
- SSL VPN (Remote Access)
- Clientless Access
- Bookmark
- Bookmark Group
- Certificate
- Certificate Authority
- Certificate Revocation Lists

Administration

Displays name of the **Administration** configurations along with number of entries:

- Settings
- Device Access
- Device Access >> Local Service ACL Exception Rule
- Updates
- Messages
- Notification
- Time
- SNMP > Agent Configuration
- SNMP > Community
- SNMP > v3 User
- Netflow

Authentication

Displays name of the **Authentication** configurations along with number of entries:

- Authentication Server
- Groups
- User
- Clientless Users
- Captive Portal
- Guest User Settings
- Guest User Settings > SMS Gateway
- Hotspots
- Hotspot Settings

System Services

Displays name of the **System Services** configurations along with number of entries:

- Web Proxy
- Authentication
- Guest User Settings
- Guest User Settings > SMS Gateway
- DoS > Settings
- DoS > Bypass Rules
- Web Content Filter > Configurations
- Web Content Filter > HTTP Scanning Rules
- Web Content Filter > HTTPS Scanning Exceptions
- Traffic Shaping Settings
- RED

- Wireless
- Advanced Threat Protection
- Malware Protection
- Log Settings
- Log Settings > Syslog Servers

Configuration

Displays name of the **Configuration** configurations along with number of entries:

- CLI Configuration
- Transparent Authentication

Objects

Assets

Displays name of the **Assets** configurations along with number of entries:

- Authentication Server
- Access Point Groups
- Web Servers

Content

Displays name of the **Content** configurations along with number of entries:

- File Type
- Custom IPS Patterns
- Custom Web Category
- URL Group
- Web App Auth Templates

Identity

Displays name of the **Identity** configurations along with number of entries:

- Certificate
- Certificate Authority
- Certificate Revocation Lists
- Groups
- User
- Clientless Users

Policies

Displays name of the **Policies** configurations along with number of entries:

- Schedule
- Access Time
- Surfing Quota
- Network Traffic Quota
- NAT
- IPSec
- IPS
- Web Filter
- Traffic Shaping
- Web App Protection
- Web App Authentication
- Device Access Profile
- Global App Traffic Shaping

- Application Group
- Hotspot Voucher Definition

Hosts and Services

Displays name of the **Hosts and Services** configurations along with number of entries:

- IP Host
- IP Host Group
- MAC Host
- FQDN Host
- FQDN Host Group
- Country Host
- Country Host Group
- Services
- Service Group

Provision Template

Click to provision the template configuration. On clicking Provision Template, Template Provision Summary window is displayed.

Template Provision Summary

Displays list of configuration entries. Select required entities and click Confirm. On clicking Confirm, Set Schedule window is displayed.

Recent Activities

Time

Displays time of the event in YYYY-MM-DD HH:MM format. The administrator can view following details for an activity: User, IP, Entity, Sub Entity, Action, Status.

Message

Details of change.

Add Template

Use the Add Device page to add new templates. Edit Template page has same parameters.

1. Go to **System Management > Device Settings > Managed Devices > Templates** and click **Add**.
2. Specify template name, which uniquely identifies the template.
3. Select the type of template to be added from the available options.

New Template

Select to store global configuration available at Firewall Manager in the form of template.

Import Device Configuration

Select to store configuration available at selected device in the form of template.

Clone Template

Select to add a new template with configuration stored in existing Template.

4. Select a device from the list of managed devices to store configuration available at that device in the form of template.
5. Select the template to be cloned.
6. Specify description of the Device.

Figure 9: Add Template

7. Click **Save**.

Provision Template

Provision Template page allows you to export a Template to Device(s). To provision a Template, refer the step shown below.

1. Go to **System Management > Device Settings > Managed Devices > Template** and click the **Provision** icon against the template to be exported.

 **Note:** You can also provision a template from **Device Configuration > Template Dashboard**.

2. Click to apply the template configuration. On clicking Apply, [Template Provision Summary](#) window is displayed.
3. Select required entities and click **Confirm** to save the settings.

Maintenance

Maintenance facilitates handling the maintenance of the managed devices.

Using the Maintenance menu, you can configure following operation:

- [Backup & Restore](#)- Allows to manually take backup or schedule backup of the managed devices.
- [Compatibility Management](#) - Allows you get the compatibility information or acquire compatibility of upcoming OS versions.
- [Inactive Users Maintenance](#) - Allows you to get report on the inactive users, also to delete the inactive users.

Backup & Restore

Use Backup & Restore page to take backup of the managed devices and store on the Firewall Manager. Firewall Manager acts as a Backup repository for device backups. Administrator can restore this backup on the device whenever required. Firewall Manager automatically takes backup of all the managed devices at the predefined intervals and if required administrator can also take backup manually.

Administrator can schedule the backup or manually take the backup from **System Management > Device Settings > Maintenance > Backup & Restore**.

Schedule Backup

Backup Frequency

Select backup frequency.

In general, it is the best to schedule backup on regular basis. Depending on how much information you add or change will help you determine the schedule.

Available options:

- Never – Select this option if you do not want to take backup
- Daily – Configure time at which the backup should be taken.
- Weekly – Configure day and time at which the backup should be taken.
- Monthly – Configure day and time at which the backup should be taken.

Backup Mode

Select backup mode.

Available options:

- Local – Select this option to store Device backup file(s) on local machine.
- FTP – Select this option if you want to store Device backup file(s) on any configured FTP server.
- FTP Server IP – Specify IP address of FTP server
- FTP Path – Specify path of backup folder on FTP server
- Username – Specify FTP server username
- Password – Specify FTP server password
- Mail – Select this option to send backup file(s) on any configured email address.

The screenshot displays a configuration window for scheduling backups. It features three main sections: 'Backup Frequency' with radio buttons for 'Never' (selected), 'Daily', 'Weekly', and 'Monthly'; 'Backup Mode' with radio buttons for 'LOCAL' (selected), 'FTP', and 'MAIL'; and a 'Devices' section containing an empty list box and an 'Add New Item' button. A blue 'Apply' button is located at the bottom left of the window.

Figure 10: Schedule Backup

Manage Backup**Select Device**

Select the Device to take backup.

Take Backup

Click to take backup of the selected Device manually.

Backup Date

Date and time in DD/MM/YYYY HH:MM:SS format on which backup was taken

Backup Type

Type of backup – Manual or Scheduled

Last Good Backup

Select a backup to be stored as ‘last good backup’. This backup will not be purged.

You can take maximum five backups including ‘last good backup’.

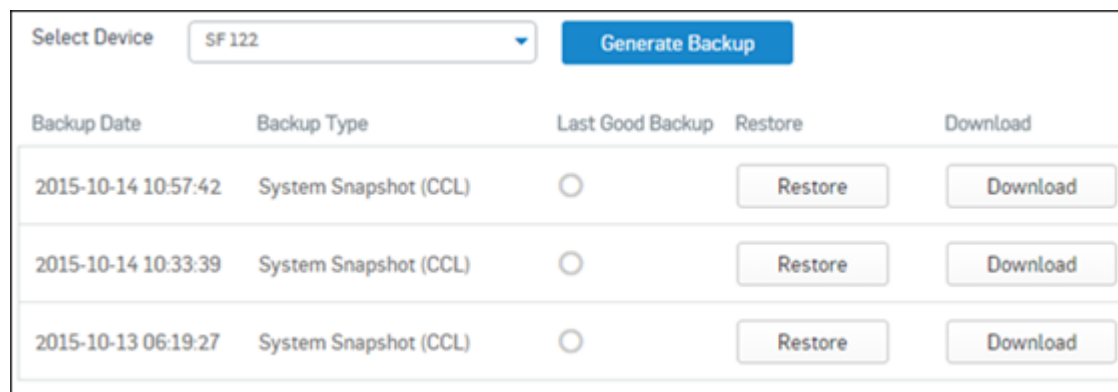
Restore

Click to restore the downloaded backup.

Download

Click to download the backup.

Maximum 5 backups of every Device will be preserved but the Last good backup will be preserved all the time.



| Backup Date | Backup Type | Last Good Backup | Restore | Download |
|---------------------|-----------------------|-----------------------|---------|----------|
| 2015-10-14 10:57:42 | System Snapshot (CCL) | <input type="radio"/> | Restore | Download |
| 2015-10-14 10:33:39 | System Snapshot (CCL) | <input type="radio"/> | Restore | Download |
| 2015-10-13 06:19:27 | System Snapshot (CCL) | <input type="radio"/> | Restore | Download |

Figure 11: Manage Backup

Compatibility Management

Firewall Manager allows the administrator to add and manage those devices which are running on newer OS versions.

As soon as a device with newer OS is discovered in Firewall Manager, Firewall Manager automatically acquires the compatibility for the newer OS version(s) from root server and displays it in the list of compatible OS versions.

This feature also enables the administrator to get the compatibility information for upcoming OS versions prior and then acquire it later.

Use this page to manage forward compatibility in Firewall Manager.

Go to **System Management > Device Settings > Maintenance > Compatibility Management** to manage compatible OS versions.

Device Compatibility Management

Default Compatibility List

Click to view the list of compatible OS versions.

Firmware

Displays list of compatible OS versions.

Compatibility Status

Displays the Compatibility status of OS version.

Available options:

Compatible Incompatible

Acquire Firmware Compatibility

Click **Enable** to acquire compatibility for the selected OS versions.

Remove Firmware Compatibility

Click **Disable** to remove compatibility of the selected OS versions.

Refresh List

Click to refresh the list of available OS versions.

Inactive User Maintenance

Inactive User Maintenance page is used to Manage Inactive Users. The following management options are available:

- Inactive Users Report – To generate and download Inactive User Reports.
- Delete Inactive Users – To delete Inactive Users.

To manage Inactive Users, go to **System Management > Device Settings > Maintenance > Inactive User Maintenance** .

Inactive Users Report

Generate Report

Specify the number of days after which the user is considered Inactive if not logged-on and the date from which the report is to be generated using calendar. Click **Generate** to generate the report.

Report

Shows the last generated Inactive Users Report. Click **Download** to download the generated reports.



Generate report for users who have not logged-on for days from 

Figure 12: Inactive Users Report

Delete Inactive Users

Specify the number of days after which the users are to be deleted if not logged-on and the start date using calendar. Click **Delete** to delete the Inactive Users.



Delete users who have not logged-on for days from 

Figure 13: Delete Inactive Users

Firmware

Use **Firmware** page to check for the latest available firmware for managed devices. To check for the availability of the latest firmware, go to **System Management > Device Settings > Firmware**.

Check for Latest Firmware

Click to check availability of latest firmware.

Model

Device Model number.

Applicable devices

Click 'List device' to view list of devices which can be upgraded with available firmware.

Applicable Version

Applicable firmware version.

Size

Size of downloadable firmware image in MB.

Type

Displays the type of firmware.

Available Options:BetaGA

Action

Click to apply downloaded firmware on the selected device(s).

Apply Firmware

Schedule

Click to schedule firmware upgrade. You can upgrade the selected device(s) with downloaded firmware immediately or you can choose to upgrade it later.

Device

Select the device to be upgraded with downloaded firmware.

Scheduled Task

Any configuration changes done on the Firewall Manager for managed devices can be applied to the device or group of device(s) immediately or can be scheduled at a later time.

Scheduled Task

Scheduled Tasks are the configurations which are to be executed at a set time or interval.

Go to **System Management > Device Settings > Schedule Task Schedule Task** to view list of task that are scheduled. You can delete or reschedule any scheduled task.

The page displays details of the task – event, entity and sub entity name, device for which task is scheduled and the schedule time.

Dynamic Objects

Dynamic objects – Host, Zone, Interface and Gateway are the network objects whose configurations vary from one device to another. Administrator can configure these objects in Firewall Manager and map them to individual devices. Administrator can use these objects while creating Firewall rule and various policies.

All of the dynamic objects are created using a similar method - create object and then specify the dynamic object-device mappings.

With dynamic objects, configuration of common objects like mail server, radius servers becomes easy as they need to be configured only once and then can be mapped.

This section covers the following topics:

- *Host* - View the list of dynamic hosts, add new hosts and manage all the configured hosts.
- *Zone* - Provides the list of all the zones including system zones and the administrator can manage the zones from this page.
- *Interface* - View port wise network (physical interface) and zone details.
- *Gateway* - Allows to manage gateway.

Host

Host is a logical building block used in defining security policies or NAT. By default, the numbers of hosts equal to the ports in the device are already created.

Host represents various types of addresses, including IP addresses, networks and Ethernet MAC addresses.

Hosts allow entities to be defined once and then be re-used in multiple referential instances throughout the configuration. For example, an internal Mail Server with an IP address as 192.168.1.15. Rather than repeated use of the IP address while constructing security policies or NAT Policies, it allows creating a single entity called "Internal Mail Server" as a Host name with an IP address as 192.168.1.15. This host, "Internal Mail Server" can then be easily selected in any configuration screen that uses Hosts as a defining criterion.

By using hosts instead of numerical addresses, you only need to make changes in a single location, rather than in each configuration where the IP address appears. Using Hosts reduces the error of entering incorrect IP addresses, makes it easier to change addresses and increases readability.

Administrator can view the list of all the dynamic hosts from **System Management > Device Settings > Dynamic Objects > Host**.

Add Dynamic Host

The **Add Dynamic Host** page allows you to manually add IP host.

1. Go to **System Management > Device Settings > Dynamic Objects > Host** and select **Add**.
2. Enter dynamic host details.

Name

Name to identify the Host.

IP Family

Select IP family of the host.

Available Options: IPv4 IPv6

Type

Select the type of host.

Available Options: Single IP Address Network IP Address with subnet IP Range

IP list to add assorted IP addresses. Use comma to specify assorted multiple IP addresses. Please note only Class B IP addresses can be added in IP list. IP addresses can be added or removed from IP list.

- MAC Address
- MAC list

Figure 14: Add Dynamic Host details

3. Enter Device - Host Mapping details.

Default

Select the host that is to be mapped with the particular device host.

Device

Select the device whose host is to be mapped with the above selected host.

Host

Select the host which is to be mapped.

Figure 15: Device-Host Mapping

4. Select **Save**.

Zone

A Zone is a logical grouping of ports/physical interfaces and/or virtual subinterfaces if defined.

Zones provide a flexible layer of security for the firewall. With the zone-based security, the administrator can group similar ports and apply the same policies to them, instead of having to write the same policy for each interface.

Default - Zone Types

LAN – Depending on the device in use and network design, one can group one to six physical ports in this zone. Group multiple interfaces with different network subnets to manage them as a single entity. Group all the LAN networks under this zone.

By default the traffic to and from this zone is blocked and hence the highest secured zone. However, traffic between ports belonging to the same zone will be allowed.

DMZ (DeMilitarized Zone) - This zone is normally used for publicly accessible servers. Depending on the device in use and network design, one can group one to five physical ports in this zone.

WAN - This zone is used for Internet services. It can also be referred as Internet zone.

VPN - This zone is used for simplifying secure, remote connectivity. It is the only zone that does not have an assigned physical port/interface. Whenever the VPN connection is established, port/interface used by the connection is automatically added to this zone and on disconnection, port is automatically removed from the zone. Like all other default zones, scanning and access policies can be applied on the traffic for this zone.

Local – Entire set of physical ports available on your device including their configured aliases are grouped in LOCAL zone. In other words, IP addresses assigned to all the ports fall under the LOCAL zone.

To manage zones, go to **System Management > Device Settings > Dynamic Objects > Zone**.

Add Dynamic Zone

This page allows you to enter zone details.

1. Go to **System Management > Device Settings > Dynamic Objects > Zone** and select **Add**.
2. Enter Dynamic Zone details.

Name

Name to identify the zone.

Type

Select Zone Type - LAN, DMZ

Available Options: **LAN** - Depending on the device in use and network design, one can group one to six physical ports in this zone. Group multiple interfaces with different network subnets to manage them as a single entity. Group all the LAN networks under this zone.



Note: By default the traffic to and from this zone is blocked and hence the highest secured zone. However, traffic between ports belonging to the same zone will be allowed.

DMZ (DeMilitarized Zone) - This zone is normally used for publicly accessible servers. Depending on the device in use and network design, one can group one to five physical ports in this zone.

Figure 16: Add Zone details



Note: By default, entire traffic will be blocked except LAN to Local zone services like Administration, Authentication and Network.

3. Enter Device-Zone Mapping details.

Default

Select the zone that is to be mapped with the particular device zone.

Device

Select the device whose zone is to be mapped with the above selected zone.

Zone

Select the zone which is to be mapped.

Figure 17: Device-Zone Mapping

4. Select **Save**.

Interface

Use **Interface** page to view port wise network (physical interface) and zone details.

If virtual subinterface is configured for the physical interface, it is also displayed beneath the physical interface. Virtual subinterface configuration can be updated or deleted.

To manage Interfaces, go to **System Management > Device Settings > Dynamic Objects > Interface**.

Add Dynamic Interface

This page allows you to configure interfaces.

1. Go to **System Management > Device Settings > Dynamic Objects > Interface** and select **Add**.
2. Enter Dynamic Interface details.

Name

Name to identify the Interface.

IP Family

Select IP Family of the Interface.

Available Options:IPv4IPv6

Type

Select Interface Type - Route and Bridge

For Route interface type you need to select Zone type:

Available Options:LAN – Depending on the device in use and network design, one can group one to six physical ports in this zone. Group multiple interfaces with different network subnets to manage them as a single entity. Group all the LAN networks under this zone.



Note: By default the traffic to and from this zone is blocked and hence the highest secured zone. However, traffic between ports belonging to the same zone will be allowed.

WAN - This zone is used for Internet services. It can also be referred as Internet zone.

DMZ (DeMilitarized Zone) - This zone is normally used for publicly accessible servers. Depending on the device in use and network design, one can group one to five physical ports in this zone.



Note: By default, entire traffic will be blocked except LAN to Local zone service likes Administration, Authentication, and Network.

Figure 18: Add Interface details

3. Enter Device-Interface Mapping.

Device

Select the device.

Interface

Select the interface which is to be mapped.

Figure 19: Device-Interface Mapping

4. Select Save.

Gateway

Device supports multiple gateways to cope with gateway failure problems. However, simply adding one more gateway is not an end to the problem. Optimal utilization of all the gateways is also necessary. Device's Multi Link Manger provides link failure protection by detecting the dead gateway and switching over to the active link and provides a mechanism to balance traffic between various links.

To manage Gateway, go to **System Management > Device Settings > Dynamic Objects > Gateway**.

Gateway Parameters

This page allows you to add a new Gateway.

1. Go to **System Management > Device Settings > Dynamic Objects > Gateway** and select **Add**.
2. Enter Dynamic Gateway details.

Name

Name to identify the Gateway.

IP Family

Select IP family of the Gateway.

Available Options:IPv4IPv6

Figure 20: Add Gateway details

3. Enter Device-Gateway Mapping details.

Device

Select the device.

Gateway

Select the gateway.

Figure 21: Device-Gateway Mapping

4. Select Save.

Change Control

Change Control page allows the administrator to view and manage list of revisions for the managed devices. Revisions are the configuration changes synchronized by the Firewall Manager and stored in Firewall Manager's repository. Each revision has a unique Change List ID. Additionally, Export Configuration can be used to export configuration and the change list of devices or device groups.

Change Control

Change Control page allows the administrator to view and manage list of revisions for the managed devices. Revisions are the configuration changes synchronized by Firewall Manager and stored in Firewall Manager's repository. Each revision has a unique Change List ID.

This page also allows the administrator to view list of affected configuration settings, compare different versions of configurations and roll back to previous configurations.

View the list of Change Control

Devices

Select the device to view configuration revisions.

Refresh Button

Click to refresh configuration revision list.

View Revision

Click to view device revision history.

Create Snapshot

Click to take snapshot of the current system configuration manually. In general, Firewall Manager takes snapshot of the system on set frequency. System Snapshot can be identified by * displayed against the entity name 'System Snapshot'.

Purge

Click to purge revision history. This option is available only for those devices which are no longer managed by Firewall Manager.

Time

Revision time in YYYY-MM-DD HH:MM format.

Change List

Unique Change List ID.

User Name

Name of the user who has done configuration changes.

IP Address

IP address of the User.

Entity

Type of Entity.

Entity Name

Name of the Entity.

Component

Name of the component used for configuration change.

Possible components:

- Central Management
- GUI
- API

Action

Action performed on the configuration.

Possible Actions:

- Update
- Insert
- Delete
- Reorder
- Enable/Disable
- Custom

Reverted Change List

Displays list of Change List IDs on mouse over. Changes associated with the listed IDs have been reverted.


Manage

Details Icon


Click  to view details of the revision. Details include listing of all dependent entities.

For example if there is a change in policy, details will display list of dependent policies.


Revert up to this change list Icon

Click  to revert the changes done in the revision.

Restore Icon

Click  to restore the configuration revision.

Purge Icon

Click  to purge the configuration revision.

View Revision History

Entity

Type of Entity

Entity Name

Name of the Entity

Time

Change List ID

Change List

Change List ID

Username

Name of the user

IP Address

IP address of the User.

Component

Name of the component used for configuration change.

Possible components:

- Central Management
- GUI
- API

Action

Action performed on the configuration.


Possible Actions:

- Update
- Insert
- Delete
- Reorder
- Enable/Disable
- Custom


Revision

Revision number. Click to view revision details.

Details Icon

Click  to view details of the revision in XML format.

Difference with Previous Version Icon

Click  to compare revision versions.

View the Change List Details**Time**

Revision time in YYYY-MM-DD HH:MM format.

User Name

Name of the user who has done configuration changes.

IP Address

IP address of the User.

Entity

Type of Entity

Component

Name of the component used for configuration change.

Possible components:

- Central Management
- GUI

- API

Action

Action performed on the configuration.


Possible Actions:

- Update
- Insert
- Delete
- Reorder
- Enable/Disable
- Custom

Revision

Revision number. Click to view revision details.

Details Icon

Click  to view details of the revision in XML format.

Difference with Previous Version Icon

Click to compare revision versions.

View Revision Details

Entity

Type of entity.

Sub Entity

Name of the sub entity.

Entity Name

Name of the entity.

Time

Revision time in YYYY-MM-DD HH:MM format.

Change List

Unique Change List ID.

Username

Name of the user who has done configuration changes.

IP Address

IP address of the User.

Component

Name of the component used for configuration change.

Possible components:

- Central Management
- GUI
- API

Action

Action performed on the configuration.

Possible Actions:


- Update

- Insert
- Delete
- Reorder
- Enable/Disable
- Custom


Revision

Revision number.

Details of change Icon

Click  to view details of the revision in XML format.

Difference with Previous Version Icon

Click  to compare revision versions.

Revert the Revision

Entity

Name of entity to be reverted.

Entity Name

Name of entity to be reverted.

Last Revision

Number of revisions. Click  to view revision details.


Action

Action to be performed on the entity.

Possible Actions:

- Update
- Insert
- Delete
- Reorder
- Enable/Disable
- Custom

Details

Click  to compare the revisions. It displays XML for current version and previous version configurations. The changes are highlighted by different color codes.

Export Configuration

Export Configuration allows the administrator to export configuration and the change list of Devices or Device groups. Multiple Devices or Device groups can be selected for export. To export configuration go to **System Management > Device Settings > Change Control Export Configuration**.

Select the Device or Device Groups from the drop down list and click **Export** to generate the configuration file in .TAR file format. To stop the export process, click **Cancel**.

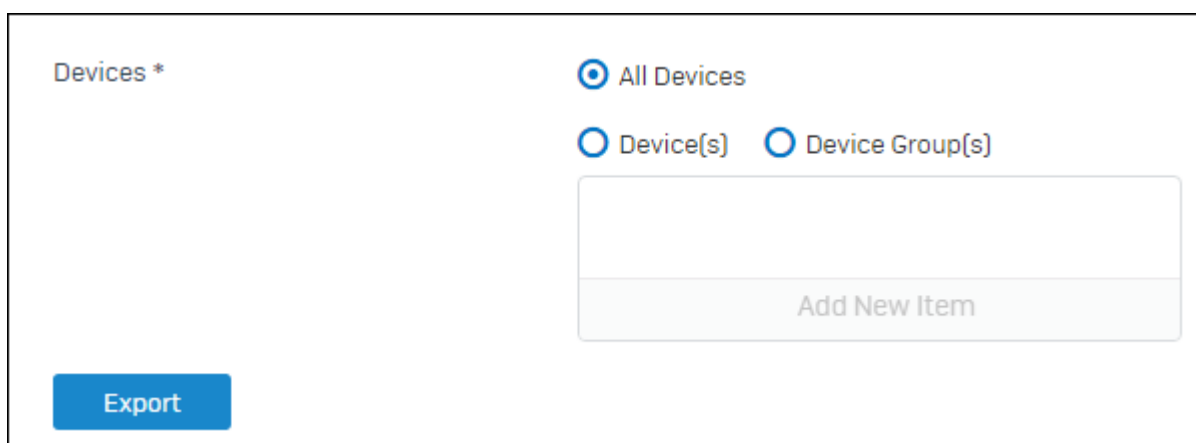


Figure 22: Export Configuration

The .TAR file contains selected Device configuration along with the change list applicable to the Device or Device group. After generating, the .TAR file can be downloaded by clicking **Download**. The .TAR file must be extracted at preferred location to view configuration details and change list details including Device Name, Device Key and Time.

Monitor

Firewall Manager helps administrator to monitor the managed devices for surfing trends, attacks and outages. Graph and Alert Profiles can be used to monitor single device or group of devices.

It normally required Administrator to log on to individual device to view system resources and information but with profiles, administrator can view that same information for all the devices from Firewall Manager itself.

Firewall Manager also provides email alerts for monitoring device in case Administrator cannot log on to Firewall Manager to monitor system resources. Alert informs when an important event occurs on an device, such as a hard disk getting too full. Dashboard Monitoring Graph displays critical health information of the managed devices in graphical manner.

Device Monitor

Dashboard Monitoring Graph displays critical health information of the managed devices in graphical manner. SFM monitors the managed Device based on the following health parameters and statuses.

Administrator can also set Dashboard Monitoring thresholds specific to Models, Devices or a graphical manner. SFM monitors the managed device based on the following health parameters and statuses:

Administrator can also set Dashboard Monitoring thresholds specific to Models, Devices or a combination of both.

Device Monitor Settings

The administrator can set the threshold values for each of the monitoring parameter. For each parameter, the administrator can provide the threshold for 'Critical' and 'Warning' states.

You can set thresholds specific to Models, Devices or a combination of both. To set the threshold values for Model/ Device/Model-Device, click **Adjust Threshold** and select among Model or Device, then click the manage icon to specify custom threshold values.

To save the values, click **Apply**.

However, if the administrator does not specify custom threshold values, the graphs are generated with Device Defaults.

Device Monitor Details

Device Monitor details page provides detailed information on the selected device card. The following information will be displayed for the device card.

Basic Information

Device Name

Displays the name the device.



Note: **Manage Device Policy** option can be used to directly take you to the device dashboard of the selected device. You can change the device policy configurations based on your observation in the Device Card.

Model Number

Displays Device Model.

Device IP

Displays the IP Address of the managed device.

Host Name

Host Name as configured on the SF device.

Security

Level and Count (Last 2 hours) are displayed for the following Security parameters:

- Web Virus
- Mail Virus
- Spam Mails
- Web Usage health
- Intrusion Attacks
- ATP Events
- Endpoint Health (Includes Red Health and missing Heartbeat)

License

Level and Status Expiry are displayed for the following License parameters:

- Base Firewall
- Network Protection
- Web Protection
- Email Protection
- Web Server Protection
- Sandstorm
- Enhanced Support
- Enhanced Plus Support
- Registered Email ID



Note: Click **Synchronize** to synchronize your device licenses.

Resource

Level Percentage and (Last 2 hours) are displayed for the following Resource parameters:

- CPU
- Memory
- Disk (Report)
- Disk (Config)

Availability

Level, Status and Duration are displayed for the following Availability parameters:

- Device Interface status

- Connection to Central Console
- Device Gateway status
- RED Status

Device Monitor

Device Monitor displays critical health information of the Managed Devices in graphical manner. SFM monitors the Managed Devices based on the following health parameters and statuses:

- Security: Mail Virus, Web Virus, Spam Mails, Web Usage Health, Intrusion Attacks, ATP Events, and Endpoint Health (Includes RED Health and missing Heartbeat).
- Resource: CPU, Memory, Disk (Report) and Disk (Config).
- License: Base Firewall, Network Protection, Web Protection, Email Protection, Sandstorm, WebServer Protection, and Support.
- Availability: Connection to Central Management, Interface status, Gateway Status and RED Status.



Note: **Connection to Central Management** parameter is not available for the auxiliary device deployed in Active-Passive HA mode.

Device Monitor continuously monitors the Managed Devices for the wide range of security attacks, resource utilization and license statuses which helps the administrator to take informed decisions in resolving the risk landscape.

Flat view and card view allows you to monitor the status (Critical, Warning, Normal) of Managed Devices across a set of parameters for Security, Resource, License and Availability, based on their threshold values. In flat view, devices that need attention are automatically listed at the top on the basis of their monitor status.

You have the flexibility to customize threshold values for Critical, Warning and Normal levels as per your needs, using Device Monitor Settings.

Open in Full Screen allows you to display Device Monitor in full screen view.

Note: **Open in Full Screen** is available only if accessed from System Management > Monitor > Device Monitor.

Graphs

Graphs menu allows you to do the following:

- [Add Profile](#)
- [View Graphs](#)

Profile

Profiles are used to generate graphs based on specific parameters. Administrator can add multiple profiles. Administrator can add profile for group of devices or single device. Tab for each profile is added on Graphs page.

Profile consists of following component:

Device: Select the devices to be included in the graph.

Category: Select from the list of categories to be included in graph.

- CPU Usage (%)
- Memory Usage (%)
- Disk Usage (%)
- Total Virus Attacks (Hits)
- Web Virus Attacks (Hits)
- Mail Virus Attacks (Hits)
- IPS Threats (Hits)
- Spam Mails (Hits)
- User Surfing Pattern (Hits)

Administrator can customize number of components for each profile.

To add or edit profile, go to **System Management > Monitoring > Graphs > Profile** and click **Add** or **Edit** Icon to modify profile details.

Profile Parameters

Title

Specify name of the profile.

Devices

Select device(s) whose details are to be displayed on the profile. If the device(s) is/are deployed in HA (High Availability) mode then it displays Primary device.

Category

Select the components to be displayed on the profile for the device(s) selected in the above field.

Available options:

- CPU Usage (%)
- Memory Usage (%)
- Disk Usage (%)
- Total Virus Attacks (Hits)
- Web Virus Attacks (Hits)
- Mail Virus Attacks (Hits)
- IPS Threats (Hits)
- Spam Mails (Hits)
- User Surfing Pattern (Hits)

If the devices are deployed in HA (High Availability) mode, the graphs for the following categories will display information for both the devices separately.

- CPU Usage (%)
- Memory Usage (%)
- Disk Usage (%)

Add Profile

Profiles are used to generate graphs based on specific parameters. Administrator can add multiple profiles. Administrator can add profile for group of devices or single device. Tab for each profile is added on Graphs page.

Profile consists of following component:

Device: Select the devices to be included in the graph.

Category: Select from the list of categories to be included in graph.

- CPU Usage (%)
- Memory Usage (%)
- Disk Usage (%)
- Total Virus Attacks (Hits)
- Web Virus Attacks (Hits)
- Mail Virus Attacks (Hits)
- IPS Threats (Hits)
- Spam Mails (Hits)
- User Surfing Pattern (Hits)

Administrator can customize number of components for each profile.

Figure 23: Add Profile

Add Profile

Graphs

To view graphs based on profiles, go to **System Management > Monitoring > Graphs > Graphs**.

If multiple profiles are added, Tab for each profile is displayed.

Depending on the components selected at the time of adding profile, profile displays line graphs for the usage status of the CPU, memory and hard disk, user surfing patten grouped into Neutral, Productive, Non Working and Unhealthy categories, virus, HTTP and mail attacks, IPS threats and spam mails.

If multiple devices are grouped under single profile, line graph of each device is plotted in each component.

Alerts

Firewall Manager allows administrator to create and send email alerts to the specified email address(es) based on predefined criteria. Firewall Manager alert notification ensures the concerned person receive an alert in situations like excess CPU, disk and memory usage or alarming count of viruses or IPS attacks.

Profile

SFM alert profile is a combination of Device(s), email address(s), and criteria to send alert notifications.

DefaultAlertProfile is a pre-configured alert profile. It can be modified but can't be deleted.

Profile page can be used to view, add or edit alert profiles. Alert Status can be disabled or enabled from the Status column itself.

Add Alert Profile

Use this page to add or edit Profile parameters.

1. Go to **System Management > Monitor > Alerts > Profile >** and click **Add** to add a new Alert Profile.
2. Specify the parameters based on description shown below.

Profile Name

Specify a name to identify the Profile.

Send Email(s) alert to

Specify comma separated recipient email address(s) to send alert notification through email.

You need to configure email server from **System Management > System Settings > System > Notification >** to send email alerts on specified email address(s).

Even if a mail server is not configured, the created alert will be displayed under **Alerts** tab.

Device(s)

Select the device(s) or device group(s).

Alerts Criteria

Configure alert criteria. Select checkbox against criterion to be configured and specify value for the criterion.

Available criteria:

- Any subscription module expires within
- CPU usage exceeds
- Memory usage exceeds
- Disk usage exceeds
- Total Intrusion attack count exceeds
- Critical Intrusion attack count exceeds
- Web virus count exceeds
- Mail Virus count exceeds
- Total virus count exceeds
- Spam Mail count exceeds
- Objectionable + Unproductive surfing hits
- ATP events exceed
- End-points with Security Heartbeat in Red state exceeds
- End-points Security Heartbeat changed to Red state exceeds
- End-points with missing Security Heartbeat exceeds
- Device connected/disconnected from central management
- Device Gateway status change
- VPN connection status change
- HA status change
- RED tunnel status change
- Hostname Change

Specify the duration of sending notifications in **Notify me** field. The duration can be in hours or minutes.

Description

Specify description of the alert profile.

Profile Name *

Description

Send email(s) alert to You can add multiple email addresses. (e.g. default@gmail.com,default@yahoo.com)

You must configure mail server to get email alerts. [Click Here](#) to update mail server settings.

Devices * Device Device Group(s)

Alerts criteria *

| | | | | | | |
|---|----------------------------------|--------------|---------------------------------|-----------|--|-----------|
| <input type="checkbox"/> Any subscription expires within | <input type="text" value="15"/> | Day(s) | | | | |
| <input type="checkbox"/> CPU usage exceeds | <input type="text" value="90"/> | % since last | <input type="text" value="20"/> | Minutes ▾ | Notify every <input type="text" value="20"/> | Minutes ▾ |
| <input type="checkbox"/> Memory usage exceeds | <input type="text" value="90"/> | % since last | <input type="text" value="20"/> | Minutes ▾ | Notify every <input type="text" value="20"/> | Minutes ▾ |
| <input type="checkbox"/> Disk usage exceeds | <input type="text" value="90"/> | % since last | <input type="text" value="20"/> | Minutes ▾ | Notify every <input type="text" value="20"/> | Minutes ▾ |
| <input type="checkbox"/> Total Intrusion attack count exceeds | <input type="text" value="500"/> | since last | <input type="text" value="30"/> | Minutes ▾ | Notify every <input type="text" value="30"/> | Minutes ▾ |
| <input type="checkbox"/> Critical Intrusion attack count exceeds | <input type="text" value="1"/> | since last | <input type="text" value="5"/> | Minutes ▾ | Notify every <input type="text" value="20"/> | Minutes ▾ |
| <input type="checkbox"/> Web Virus count exceeds | <input type="text" value="20"/> | since last | <input type="text" value="30"/> | Minutes ▾ | Notify every <input type="text" value="30"/> | Minutes ▾ |
| <input type="checkbox"/> Mail Virus count exceeds | <input type="text" value="20"/> | since last | <input type="text" value="30"/> | Minutes ▾ | Notify every <input type="text" value="30"/> | Minutes ▾ |
| <input type="checkbox"/> Total Virus count exceeds | <input type="text" value="20"/> | since last | <input type="text" value="30"/> | Minutes ▾ | Notify every <input type="text" value="30"/> | Minutes ▾ |
| <input type="checkbox"/> Spam Mail count exceeds | <input type="text" value="50"/> | since last | <input type="text" value="30"/> | Minutes ▾ | Notify every <input type="text" value="30"/> | Minutes ▾ |
| <input type="checkbox"/> Objectionable + Unproductive surfing hits exceeds | <input type="text" value="300"/> | since last | <input type="text" value="30"/> | Minutes ▾ | Notify every <input type="text" value="30"/> | Minutes ▾ |
| <input type="checkbox"/> ATP Events exceeds | <input type="text" value="1"/> | since last | <input type="text" value="5"/> | Minutes ▾ | Notify every <input type="text" value="20"/> | Minutes ▾ |
| <input type="checkbox"/> End-points with Security Heartbeat in Red state exceeds | <input type="text" value="20"/> | % | | | Notify every <input type="text" value="30"/> | Minutes ▾ |
| <input type="checkbox"/> End-points Security Heartbeat changed to Red state exceeds | <input type="text" value="20"/> | % in last | <input type="text" value="60"/> | Minutes ▾ | Notify every <input type="text" value="60"/> | Minutes ▾ |
| <input type="checkbox"/> End-points with missing Security Heartbeat exceeds | <input type="text" value="5"/> | % | | | Notify every <input type="text" value="30"/> | Minutes ▾ |
| <input type="checkbox"/> Device connected/disconnected from Central Management | | | | | | |
| <input type="checkbox"/> Device Gateway status change | | | | | | |
| <input type="checkbox"/> VPN connection status change | | | | | | |
| <input type="checkbox"/> HA status change | | | | | | |
| <input type="checkbox"/> RED tunnel status change | | | | | | |
| <input type="checkbox"/> Hostname Change | | | | | | |

Figure 24: Add Alert Profile

3. Click Save.

Alerts

Firewall Manager allows you to view the list of generated alerts based on configured alert profiles. You can view these alerts from **System Management > Monitor > Alerts > Alerts** .

Event Viewer

Audit and System logs are an important part of any secure system that provides a comprehensive view into the current and past state of almost any type of complex system, and they need to be carefully designed in order to give a faithful representation of system activity.

They can identify what action was taken by whom and when. The existence of such logs can be used to enforce correct user behavior, by holding users accountable for their actions as recorded in the audit log. They are the simplest, yet also one of the most effective forms of tracking temporal information. The idea is that any time something significant happens you write some record indicating what happened and when it happened.

Device Events

Device Events page allows you to do the following operations:

- **View:** Load archived file to view and search. Click checkbox against the file and click View Data link, which opens a new page from where you can search the log. This process may take some time depending on the size of data. Note that this option is available if and only if Sophos iView is integrated with Firewall Manager. To configure iView integration, go to **System Management > System Settings > Administration > iView > .**
- **Unload:** Unload archived file. Click against the file to be unloaded.
- **Search Archived Logs:** Perform a refined search based on multiple criteria.



Search Archived Logs

Search Archived log page allows you to perform a refined search based on multiple criteria.

1. Go to **System Management > Monitoring > Event Viewer > Device Events >** and click the **View Data** link.
2. Under **Advanced Search**, select **Match all of the following** to get search result based on all criteria or **Match any of the following** to get search result based on any of the specified criterion.
3. Add searching criterion from the available options.

Available options:

Upload Time
Log Component
Status
Username
IP address
Message

The search can be performed using multiple search criteria. Click  to add a new search criterion and  to remove a search criterion.

4. Click **Search** to perform the search or **Clear All** to reset.
5. Select the view for search result display.

Possible options:

Graphs – Displays logs in graphical format. This option is available for following file types:

- System Logs
- Anti Virus
- IPS
- Authentication
- Audit Logs
- Anti Virus
- IPS

Formatted Logs: Displays logs in syslog format.

Raw Logs: Displays logs in syslog format.

View Graphical Search Results – Anti Virus**Top Viruses Graph**

Graph displays number of counts per protocol.

Top Web Viruses

Graph displays number of counts per web virus.

Top FTP Viruses

Graph displays number of counts per FTP virus.

Top Mail Viruses

Graph displays number of counts per mail virus.

View Graphical Search Results – IPS**Top Attacks Graph**

Graph displays number of counts per attack.

Top Attackers Graph

Graph displays number of counts per attacker IP address.

Top Victims Graph

Graph displays number of counts per victim IP address.

Top Users Graph

Graph displays number of counts per User.

Device Logs

Device Logs page allows to view the logs for modules like Application Filter, Web Filter, Anti Spam and Firewall. This page gives consolidated information about all the events that have occurred.

To view logs of any of the managed Device, go to **System Management > Monitoring > Event Viewer > Device Logs >** and select module and Device.

Available Log Modules:

- Web Filter – Web Filter logs provide information about the users that were detected accessing restricted URLs and the action taken by the managed Device.
- Application Filter – Application Filter logs provide information about applications to which access was denied by the managed Device.
- Anti Spam – Anti Spam logs provide information about the spam mails identified by managed Device.
- Firewall – Firewall logs provide information about how much traffic passes through a particular rule and through which interfaces.
- Authentication – Authentication logs provide information about all the authentication logs including Firewall, VPN and My Account authentication.
- Web Server Protection [WAF] – Web Server Protection [WAF] logs provide information about HTTP/S requests and action taken on the same.
- Advanced Threat Protection - Advanced Threat Protection provide information about advanced malwares detected.

Management System Events

Event Viewer page allows to view the events for various modules – Policy Configuration, System, System Events. This page gives consolidated information about all the events that occurred for the respective modules and information can be filtered based on Event ID, Username or IP address.

To view Firewall Manager events, go to **System > Monitoring > Event Viewer > Management System Events >** , select date and any of the following modules:

- Policy Configuration Events – Provides information of the administrative events and task occurred at global and device level.
- System Management – Provides information of the administrative events and task occurred at Firewall Manager.
- System Events– Provides information of the system events and tasks occurred at Firewall Manager.



Note: In the combined filter for User Name and IP Address, you can enter value in either one of them or a combination of both.

System Settings

System Settings allows configuration and administration of SFM Device for secure and remote management as well as administrative privilege that you can assign to admin users. It also provides the basic system settings of the Web Admin console. Configuration of several non-network features, such as SNMP, custom messages, portal setting and themes can also be done through System. System also allows basic configuration of SFM including GUI localization, mail server, customized messages, web & parent proxy settings, themes and outlook for the Captive portal. You can also configure Network entities, Firmware, Signatures and Diagnostic utilities for Firewall Manager using System Settings.

Administration

Administration covers general configuration of Firewall Manager including adding administrators. You can configure administrative access settings including login parameters and port settings. You can also create new users and view all active users. Using Access Profile, you can enable role-based administration capabilities to offer greater granular access control and flexibility. Additionally, Administration allows you configure Sophos iView and API Explorer settings.

Settings

Use **Settings** page to configure administrative access settings. The page also allows you to configure localization, signature port and change control settings.

To manage the administration settings, go to **System Management > System Settings > Administration > Settings >** .

Web Admin Settings

HTTP Port

Provide the port number to configure HTTP Port.

By default, the HTTP Port number is 80.

HTTPS Port

Provide the port number to configure HTTPS Port for Secured Web Admin Console access.

By default, the HTTP Port number is 443.

Syslog Port

Displays Syslog port number configured to communicate with managed SF device(s).

Syslog (Secure)

Displays Secure Syslog port number configured to communicate with managed SF device(s).

Certificate

Certificate that will be used by Administrator of Firewall Manager Web Admin Console.

| | |
|------------------|---|
| HTTP Port * | <input type="text" value="80"/> |
| HTTPS Port * | <input type="text" value="443"/> |
| Syslog Port * | <input type="text" value="514"/> |
| Syslog(Secure) * | <input type="text" value="6514"/> |
| Certificate * | <input type="text" value="ApplianceCertificate"/> |

Figure 25: Web Admin Settings

Content Distribution Port Settings

Content Distribution Port

Provide the port number to distribute updates for pattern.

| | |
|---------------------------|-----------------------------------|
| Content Distribution Port | <input type="text" value="8443"/> |
|---------------------------|-----------------------------------|

Figure 26: Content Distribution Port Settings

Administrator Password Complexity Settings

Password Complexity can be configured to ensure that administrators are using secure passwords.

- Enable Password Complexity Settings to enforce following constraints:
- Minimum Password length. Configure minimum characters required in the password. By default, the Minimum Password length is eight (8) characters.
- Require minimum one Upper and lower case alphabet
- Require minimum one number i.e. 0 - 9
- Require at least one special character e.g. @, \$, %
- Password cannot be same as username.

| |
|---|
| <input type="checkbox"/> Enable Password Complexity Check |
| <input type="checkbox"/> Minimum Password length should be of <input type="text" value="8"/> characters |
| <input type="checkbox"/> Include atleast 1 each Upper and Lower case alphabetic characters |
| <input type="checkbox"/> Include atleast 1 numeric character |
| <input type="checkbox"/> Include atleast 1 special character like '@', '\$', '!', etc |
| (Note: Password must not be a User Name) |

Figure 27: Administrator Password Complexity Settings

All the enabled constraints are applied to administrator user password.

Change Control Settings

Enable Change Control

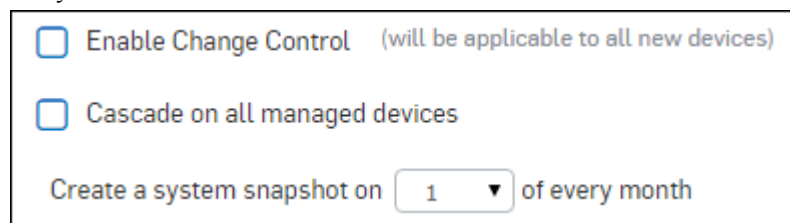
Click to enable Change Control in devices which will be added to Firewall Manager .

Cascade on all managed devices

Click to enable Change Control in all existing managed devices.

Create a system snapshot on of (X) every month

Specify the date on which you want to auto-generate System Snapshot. If you specify "5", Firewall Manager will auto-generate system snapshot on 5th date of every month. Default value is 1st date of every month.



Enable Change Control (will be applicable to all new devices)

Cascade on all managed devices

Create a system snapshot on of every month

Figure 28: Change Control Settings

Sophos Adaptive Learning

The product sends information periodically to Sophos which is used for the purpose of improving stability and protection effectiveness, and prioritizing feature refinements. It includes configuration and usage information, and monitoring threshold data.

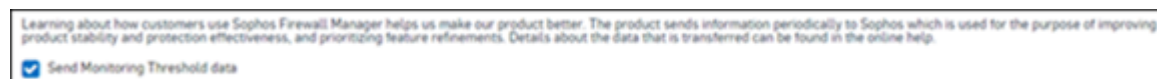
Configuration and usage data such as Device information (e.g. model, hardware version), Firmware and License information, Features in use [status, on / off, count] (e.g. configuration applied to 1 or more devices, signature distribution status), amount of configured objects and items (e.g. count of managed devices and groups, count of hosts, policies), Product errors, CPU, memory and disk usage (in percentage), is collected by default.

No user-specific information or personalized information is collected. The information is transmitted to Sophos over HTTPS.

Send Monitoring Threshold data

Monitoring Threshold data includes (enabled by default, excluded when option is de-selected) the following to improve the default threshold settings and alert criteria given with the product across models:

- Monitoring Threshold values per model.
- Alert threshold criteria/values per model.



Learning about how customers use Sophos Firewall Manager helps us make our product better. The product sends information periodically to Sophos which is used for the purpose of improving product stability and protection effectiveness, and prioritizing feature refinements. Details about the data that is transferred can be found in the online help.

Send Monitoring Threshold data

Figure 29: Sophos Adaptive Learning

Disk Usage Alerts

Use the settings below to configure sending automatic email alerts to a specified email address, when the hard disk usage of your SFM device exceeds the specified threshold value.

Send Email Alert

Select this to receive email alerts when disk usage exceeds configured **Disk Usage Threshold**.

Disk Usage Threshold

Enter disk usage threshold value in percentage above which email alerts should be sent.

Current Disk Usage

Displays current available used disk space in percentage.

Send Email Alert

You must configure mail server to receive email alerts. [Click here](#) to configure mail server.

Disk Usage Threshold %

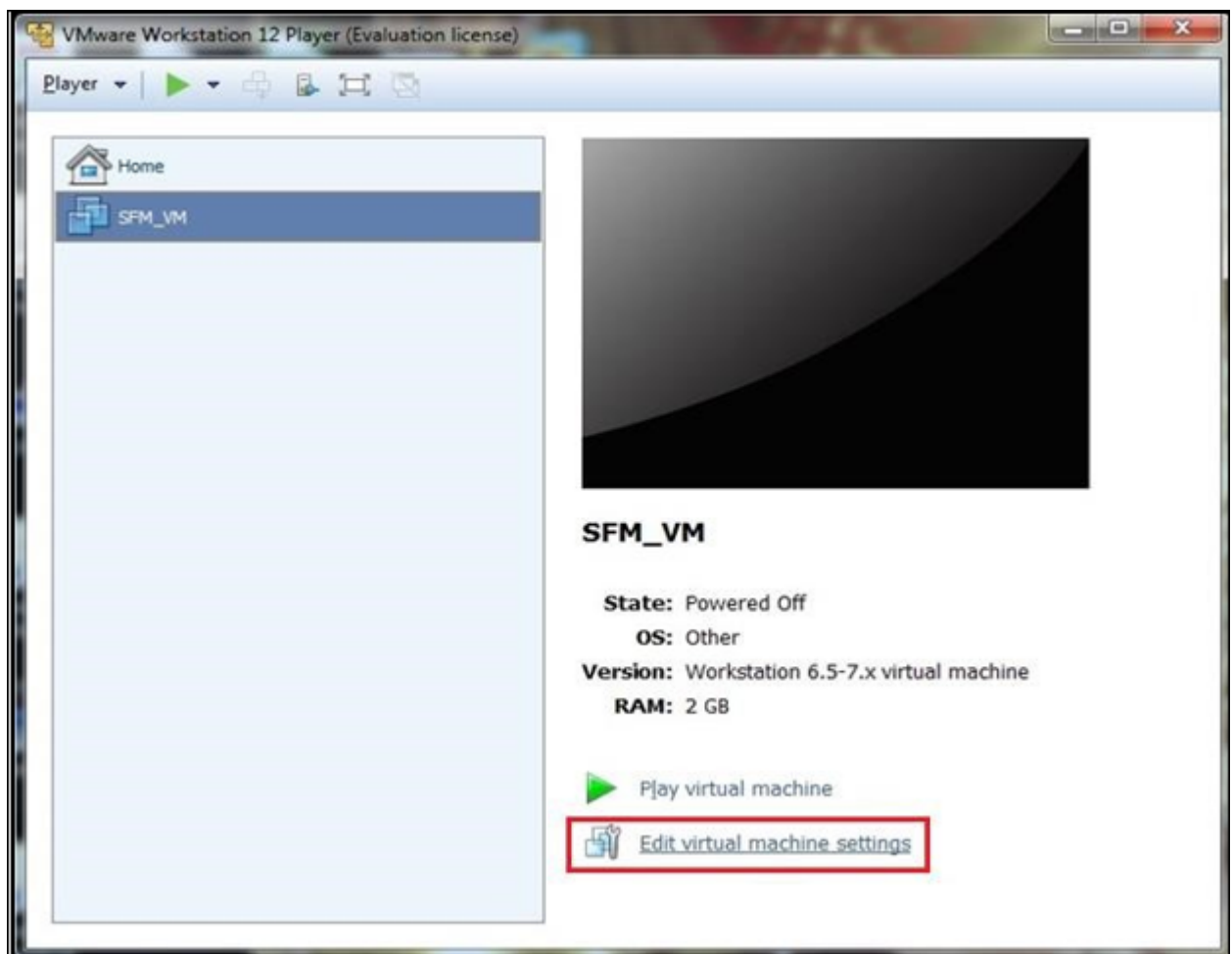
Current Disk Usage %

Note: Three emails will be sent one per day after disk usage exceeds configured Threshold Value.

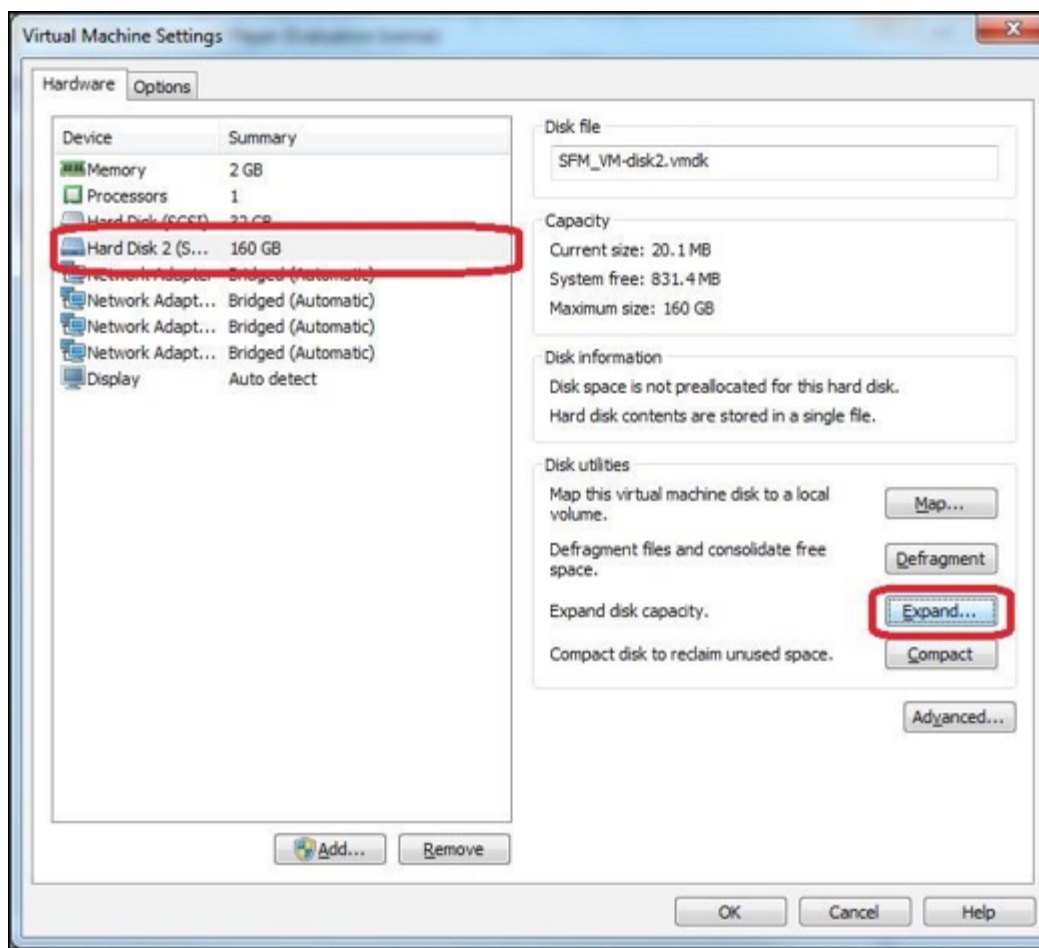
For virtual SFM once the disk usage exceeds the configured Threshold Value you can increase the size of disk, follow below steps to do so for various virtual machines:

1. VMware Virtual Machine:

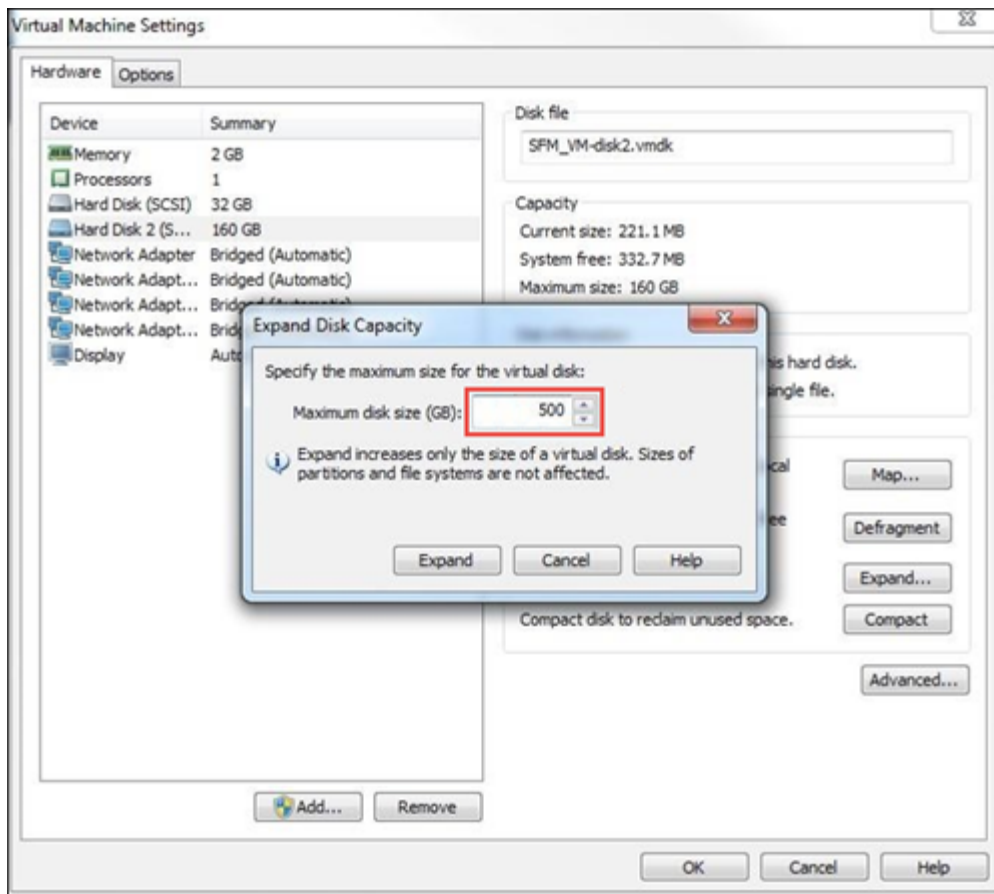
- a. Open VMware Virtual Machine where SFM is deployed.
- b. Click **Edit virtual machine settings**.



- c. Click Hard Disk 2 then click on **Expand...**

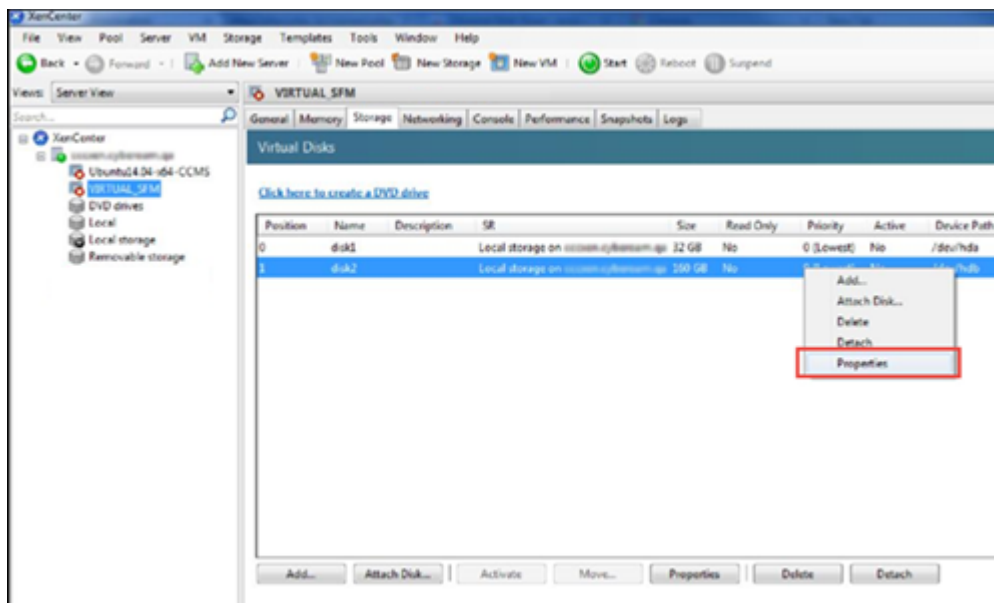


d. Enter **Maximum disk size** as required and click **Expand**.

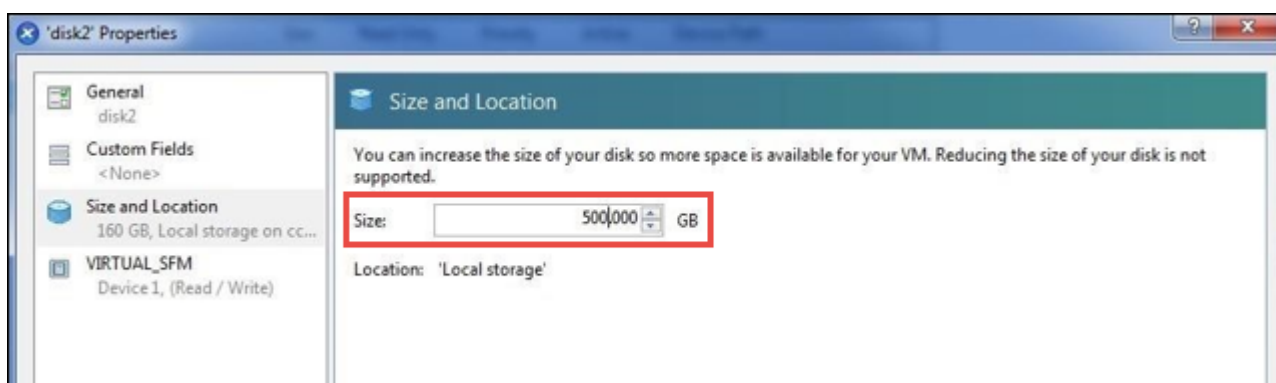


2. Xen Virtual Machine:

- a. Open Xen virtual machine where SFM is deployed.
- b. Switch to **Storage** tab, right click on disk-2 and select **Properties**.



- c. Click on **Size and Location**.
- d. Update disk size as required.



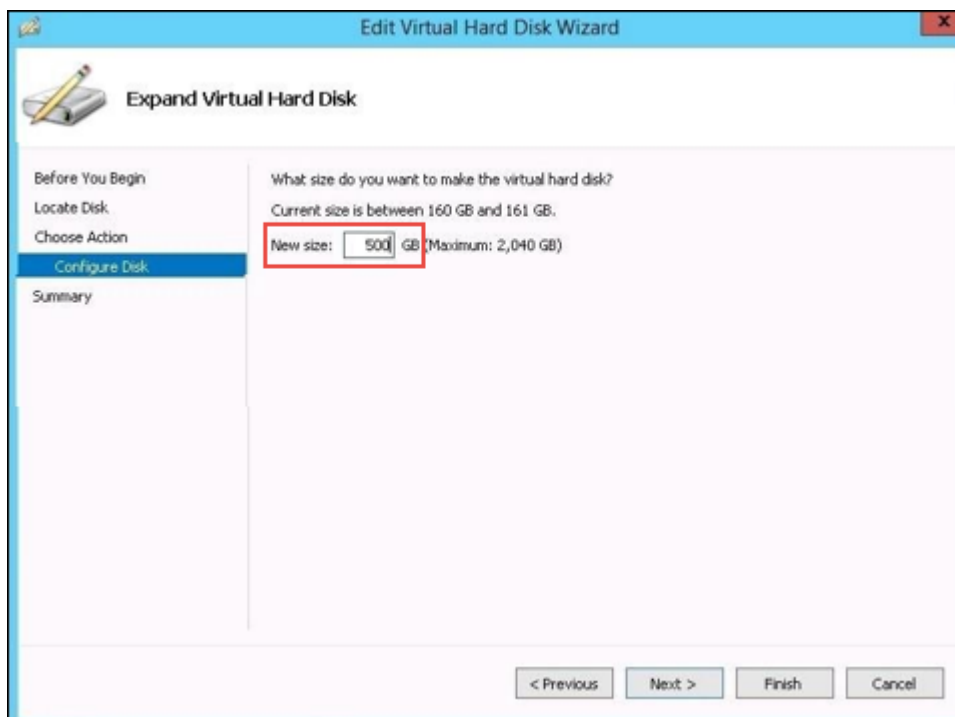
- e. Click on **OK** to save.
3. **KVM:** Disk size for KVM can be increased by using the following command:


```
qemu-img resize AUXILIARY-DISK.qcow2 +(disk_size)GB
```

To execute this command, navigate to 'AUXILIARY-DISK.qcow2' file. For example if your file is stored in SFM folder then navigate to SFM (/home/SFM/) and execute the command (qemu-img resize AUXILIARY-DISK.qcow2 +500 GB).

4. Hyper-V virtual machine:

- a. Open Hyper-V virtual machine where SFM is deployed.
- b. Go to **File > Settings**.
- c. Select IDE Controller1 Auxiliary Hard disk and click on **Edit**.
- d. Go to **Choose Action > Configure Disk**.
- e. Update disk size as required and click on **Finish**.



 **Note:** For hardware SFM devices the disk size cannot be increased.

Access Profile

Use the **Access Profile** page to create profiles for Administrators. Role-based administration capabilities are provided to offer greater granular access control and flexibility. Profile sets up access levels for the administrative users. Profile determines the privileges of the administrator and the administrator's access to managed SF Device and SFM features.

Access profile page is divided into access control categories for which you can enable None, Read-only, or Read-Write access. For ease of use by default, SFM Device is shipped with profile "Administrator" with full privileges and "Device Administrator" with privileges over specific Devices.

To manage default and custom profiles, go to **System Management > System Settings > Administration > Access Profile >** .



Note:

- You cannot delete the default profiles.
- You cannot delete profile assigned to any user.

You can view added profiles, [add new profiles](#) or edit or delete existing profiles.

Add Access Profile

Use this page to add an Access Profile.

1. Go to **System Management > System Settings > Administration > Access profile >** and click **Add**.
2. Enter Profile details.

Profile Name

Name to identify the profile. By default Firewall Manager is shipped with two profiles.

- Administrator – super administrator with full privileges device
- device Administrator – read-write privileges for selected device(s)


Configuration

Click on the access level you want to provide to a profile. There are three levels of access each of the created profile can have.

Available Options:

None: No access to any page **Read-Only:** View the pages **Read-Write:** Modify the details

Access levels can be set for individual menus as well. You can either set a common access level for all the menus or individually select the access level for each of the menu.

Click  icon against a menu to view the items under that menu.

For example, if you set access level as Read-Only against the Web Filter, the profile user would only be able to view the Web Filter menu but would not be able to make any modifications.

To make modifications, Read-Write option is to be used.

Profile Name *

None
 Read-Only
 Read-Write

Device Configuration

| | | | |
|--|----------------------------------|-----------------------|-----------------------|
| Dashboard | <input checked="" type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Objects | <input checked="" type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Network | <input checked="" type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Firewall | <input checked="" type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Console Access From GUI | <input checked="" type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Web Filter | <input checked="" type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Application Filter | <input checked="" type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Traffic Shaping | <input checked="" type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Traffic Discovery | <input checked="" type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| <input checked="" type="checkbox"/> System | <input checked="" type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| <input checked="" type="checkbox"/> Identity | <input checked="" type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| <input checked="" type="checkbox"/> VPN | <input checked="" type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| <input checked="" type="checkbox"/> IPS | <input checked="" type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| <input checked="" type="checkbox"/> AV | <input checked="" type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| <input checked="" type="checkbox"/> AS | <input checked="" type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| <input checked="" type="checkbox"/> Logs & Reports | <input checked="" type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| <input checked="" type="checkbox"/> Web Server Protection(WAF) | <input checked="" type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| <input checked="" type="checkbox"/> Wireless Protection | <input checked="" type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| System Management | | | |
| <input checked="" type="checkbox"/> System Settings | <input checked="" type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| <input checked="" type="checkbox"/> Device Settings | <input checked="" type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| <input checked="" type="checkbox"/> Monitor | <input checked="" type="radio"/> | <input type="radio"/> | <input type="radio"/> |

Figure 30: Add Profile

3. Click **Save**.

Users

Use the **Users** page to add administrators. It allows configuring administrator access to the SF device, including the level of access and which devices administrator have access to. All administrator settings can be configured only when you are logged in as the admin administrator. The admin administrator is the only user with complete access to the entire Firewall Manager device options.

To manage users, go to **System Management > System Settings > Administration > Users >** .

You can view added users, [add new users](#) or edit or delete existing users.

Add User

1. Go to **System Management > System Settings > Administration > Users >** and click **Add** to register a new user.
2. Specify user details based on the description shown below.

Username

Specify username, which uniquely identifies user and will be used for login.

Authentication Type

Select type of authentication for the user:

- Local
- External – LDAP, Radius, TACACS+

Refer Authentication Server page for details.

Status

Select the status of the user.

Available Options:

- Active
- Inactive

Password/Confirm Password

Specify Password for the user.

Email ID

Specify Email address of the user.

Access Profile

Select the Profile.

Administrator will get access of various Web Admin console menus as per the configured profile.

You can create a new profile directly from this page itself and attach to the user.

Accessible Device

Select the device to be assigned to the user.

Device Group

Select the Device Group for the user. The user will be able to manage all devices in the group, in addition to the individual devices selected earlier.



Note: Only Super Administrator of Firewall Manager will be able to assign or update device groups.

| | |
|-----------------------|--|
| User Name * | <input type="text" value="Enter UserName"/> |
| Authentication Type * | <input checked="" type="radio"/> Local <input type="radio"/> External |
| Status * | <input checked="" type="radio"/> Active <input type="radio"/> Inactive |
| Password * | <input type="text" value="Password"/> <input type="text" value="Confirm Password"/> |
| Email * | <input type="text" value="Enter Email Address"/> |
| Access Profile * | <input type="text" value="Device Administrator"/> |
| Accessible Device | <input type="text"/> <input type="button" value="Add New Item"/> |
| Device Group | <input type="text"/> <input type="button" value="Add New Item"/> |

Figure 31: Add User

3. Click Save.

Device Access

Device access allows limiting the Administrative access of the following device services from various ports:

- HTTP
- HTTPS
- Telnet
- SSH
- Ping
- Syslog
- Syslog (Secure)

To manage access to device, go to **System Management > System Settings > Administration > Device Access**.

Default Access Control Configuration

When Firewall Manager is connected and powered up for the first time, it will have a default access configuration. HTTP, HTTPS, Telnet, SSH, Ping, Syslog services will be enabled for administrative functions from Port A and B.

Custom Access Control Configuration

Use access control to limit the access to Firewall Manager for administrative purposes. Enable/disable access to Firewall Manager using following services from the specified port: HTTP, HTTPS, Telnet, SSH, Ping, Syslog, Syslog (Secure).

Live Users

Live Users page displays list of currently logged on users and their important parameters. Use Live User page to manage live users of Firewall Manager.

To manage live users, go to **System Management > System Settings > Administration > Live Users >** .

iView

iView page allows administrator to configure Sophos iView as centralized reporting server for all managed Devices.

To configure iView as the reporting server, refer the steps shown below.

1. Go to **System Management > System Settings > Administration > iView >** and click **Enable iView Integration** .
2. Specify the iView Server details based on the description shown below.

Username

Displays Username of iView administrator user i.e. admin. This field cannot be updated.

Password

Specify password of iView administrator user.

Re-enter the password to confirm.



Note: Password can only be edited if **Enable iView Integration** is selected.

iView internal IP address

Specify LAN IP address of iView Web Admin Console.

Web Admin Port

Specify port number to access iView Web Admin Console over LAN.

iView external IP address

Specify WAN IP address of iView Web Admin Console.

Web Admin Port

Specify port number to access iView Web Admin Console over Internet.

Select Syslog Server

Select Syslog Server to send log data of all managed Devices. The syslog server can be configured from **Policy > System > Configuration > Log Settings > Syslog Servers**.

Sync Configuration Changes only

Click to synchronize only newly added or updated entries immediately.

Sync Full Configuration

Specify the time interval at which entire device-user repository will be synchronized.

3. Click **Apply**.

API Explorer

Application Programming Interface (API) is an interface which allows third party applications to communicate with Firewall Manager.

This page enables the administrator to access Firewall Manager's XML based API to retrieve a certain set of information from Firewall Manager.

Firewall Manager API supports 'get' API request type to retrieve the information.

To access Firewall Manager API, go to **System Management > System Settings > Administration > API**.

API Explorer**API Request**

Write the API query. Based on the API query, API response will be displayed.

Submit

Click to submit XML query.

API Response

Displays response of submitted XML query.

System

Use **System** pages to configure mail server, set administrator email ids, set system date and time and NTP server.

This section covers the following topics:

- [Certificate](#) - Use to generate self-signed certificate or upload a certificate.
- [Authentication Server](#) - Use to manage authentication server.
- [Authentication Preferences](#) - Allows to set preference for authentication server(s) to decide the order in which they will be used.
- [Notification](#) - Allows to configure mail-server settings.
- [Time](#) - Use to configure time settings.
- [HA](#) - Use to configure or disable HA.

Certificate

Certificate page allows you to upload a certificate. A digital certificate is a document that guarantees the identity of a person or entity and is issued by the Certificate Authority (CA). Certificates are generated by the third party trusted CA. They create certificates by signing public keys and identify the information of the communicating parties with their own private keys. This way it is possible to verify that a public key really belongs to the communicating party only and not been forged by someone with malicious intentions.

Certificate page allows you to upload third party certificate. To manage Certificates, go to **System Management > System Settings > System > Certificate**.

Add Certificate

Use the **Add Certificate** page to add new certificate.

1. Go to **System Management > System Settings > > System > Certificate** and click **Add**.
2. Specify Certificate details based on the given description.

Name

Name to identify the Certificate.

Password

Password for a Certificate used for authentication.

Confirm Password

Re-enter password for confirmation.

Certificate

Specify certificate to be uploaded. Use Browse to select the complete path.

Private Key

Specify private key for the certificate. Use Browse to select the complete path.

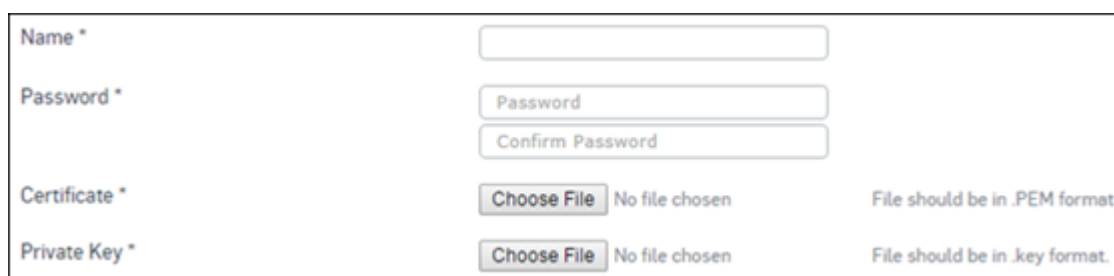


Figure 32: Upload Certificate

3. Click **OK**.

Authentication Server

Device supports user authentication against:

- a LDAP Server
- a RADIUS Server
- an internal database defined in Device

User authentication can be performed using local user database, RADIUS, LDAP or any combination of these.

Local Authentication

Device provides a local database for storing user information. You can configure device to use this local database to authenticate users and control their access to the network. Choose local database authentication over LDAP or RADIUS when the number of users accessing the network is relatively small. Registering dozens of users takes time, although once the entries are in place they are not difficult to maintain. For networks with larger numbers of users, user authentication using LDAP or RADIUS servers can be more efficient.

Combination of external and local authentication is useful in large networks where it is required to provide guest user accounts for temporary access while a different authentication mechanism like RADIUS for VPN and SSL VPN users provides better security as password is not exchanged over the wire.

External Authentication

External Authentication Servers can be integrated with the device for providing secure access to the users of those servers.

To manage external authentication servers, go to **System Management > System Settings > System > Authentication Server**.

Add Authentication Server

To manage external authentication servers, go to **System Management > System Settings > System > Authentication Server** and select **Add**.

Server Type

Select the service with which you want to use your network.

Available Options: *LDAP Server* *RADIUS Server* *TACACS+ Server*

Configure LDAP Server

When device is installed in Windows environment with LDAP server, it is not necessary to create users again in the device. device provides a facility to automatically create user(s) on first logon. Whenever the existing user(s) in LDAP logs on for the first time after configuration, user is automatically created in the device and is assigned to the default group.

This reduces Administrator's burden of creating the same users in the device.

User has to be authenticated by device before granting access the Internet. device sends the user authentication request to LDAP and LDAP server authenticates user as per supplied tokens. User can log on using their Windows authentication tokens.

1. Go to **System Management > System Settings > System > Authentication Server** and select **Add**.
2. Select Server Type as LDAP Server. If user is required to authenticate using an LDAP server, device needs to communicate with LDAP server for authentication.
3. Enter LDAP details.

Server Name

Name to identify the server.

Authentication Server IP

Specify LDAP Server IP address.

Port

Specify Port number through which Server communicates.

Default port is 389.

Version

Select LDAP version. For example, 2. Default value is Version 3.

Base DN

Specify the base distinguished name (Base DN) of the directory service, indicating the starting point for searching user in the directory service. If you are not aware about Base DN, click Get Base DN to retrieve base DN.

The top level of the LDAP directory tree is the base, referred to as the "Base DN". A base DN usually takes one of the three forms: Organization name, Company's Internet Domain name or DNS domain name. For example dc=google, dc=com

Administrator

Specify Username for the user with Administrative privileges for LDAP server.

Password

Specify Password for the user with Administrative privileges for LDAP server

Authentication Attribute


Set authentication attribute. It is the attribute used to perform user search.

By default, LDAP uses uid attribute to identify user entries. If you want to use a different attribute (such as given name), specify the attribute name in this field.

| | | |
|----------------------------|--------------------------------|-----------------------------|
| Server Type | LDAP Server ▼ | |
| Server Name * | Enter Server Name | |
| Authentication Server IP * | Enter Server IP | |
| Port * | 389 | |
| Version * | 3 ▼ | |
| Base DN * | Enter Base DN | Get Base DN |
| Administrator * | Enter ADS Username | |
| Password * | Password | |
| Authentication Attribute * | Enter Authentication Attribute | |

Figure 33: Add LDAP Server

4. Click **Test Connection** button to check the connectivity between LDAP and the device.
5. Click **Save**.

 **Note:** Whenever the existing user(s) in LDAP logs on, user is automatically created in the device and assigned to the default group.

Configure RADIUS Server

RADIUS stands for Remote Authentication Dial In User Service and is a protocol for allowing network devices to authenticate users against a central database. In addition to user information, RADIUS can store technical information used by network devices such as protocols supported, IP addresses, telephone numbers, routing information, and so on. Together this information constitutes a user profile that is stored in a file or database on the RADIUS server.

RADIUS servers provide authentication, authorization, and accounting functions but device uses only the authentication function of the RADIUS server.

Before you can use RADIUS authentication, you must have a functioning RADIUS server on the network.

1. Go to **System Management > System Settings > System > Authentication Server** and select **Add**.
2. Select Server Type as RADIUS Server. If user is required to authenticate using a RADIUS server, device needs to communicate with RADIUS server for authentication.
3. Enter the details.

Server Name

Name to identify the RADIUS Server.

Server IP

Specify RADIUS Server IP address.

Authentication Port

Specify port number through which server communicates.

Default port - 1812

Shared Secret

Specify share secret, which is to be used to encrypt information passed to the device.

| | |
|-----------------------|-------------------|
| Server Type | RADIUS Server ▼ |
| Server Name * | Enter Server Name |
| Server IP * | Enter Server IP |
| Authentication Port * | 1812 |
| Shared Secret * | Shared Secret |

Figure 34: Add RADIUS Server

4. Click **Test Connection** button to check the connectivity between RADIUS and the device.
5. Click **Save**.

 **Note:** Whenever the existing user(s) in RADIUS logs on, user is automatically created in device and assigned to the default group.

Configure TACACS+ Server

TACACS+ (Terminal Access Controller Access Control System Plus) provides access control for routers, network access servers and other networked computing devices via one or more centralized servers.

TACACS+ provides separate authentication, authorization and accounting services but the device uses only the authentication function of the TACACS+ server.

Before you can use TACACS+ authentication, you must have a functioning TACACS+ server on the network.

1. Go to **System Management > System Settings > System > Authentication Server** and select **Add**.
2. Select Server Type as TACACS+ Server. If the user is required to authenticate using a TACACS+ server, device needs to communicate with TACACS+ server for authentication.
3. Enter the details.

Server Name

Enter name to identify the TACACS+ Server.

Server IP

Specify TACACS+ Server IPv4 Address.

Port

Specify port number on the TACACS+ server to which the device sends the authentication request.

Default - 49

Shared Secret

Provide shared secret, which is used to encrypt information passed to the device.

| | |
|-----------------|-------------------|
| Server Type | TACACS+ Server ▼ |
| Server Name * | Enter Server Name |
| Server IP * | Enter Server IP |
| Port * | 49 |
| Shared Secret * | Shared Secret |

Figure 35: Add TACACS+Server

4. Click **Test Connection** button to check the connectivity between TACACS+ and the device.
5. Click **Save**.



Note:

- Device supports CHAP & PAP authentication methods to authenticate L2TP/PPTP users against TACACS+ server.
- Device supports PAP authentication protocol to authenticate Firewall/Administrator/VPN users against TACACS+ server.

Authentication Preferences

You can set preference for authentication server(s) to decide the order in which they will be used. Set preferences for added external servers from **System Management > System Settings > System > Authentication Preferences**.

Enter External Authentication Server details.

Authentication Servers List

Select authentication server from Authentication Servers list. Selected servers will be displayed under 'Selected Authentication Server' list.



Note:

Figure 36: Authentication Preference

- Selected Authentication Server list order displays preferences.
- Do not forget to click Apply after adding.

Notification

Configure mail server IP address, port and email address where the Firewall Manager has to send and receive alert emails.

To configure mail server settings, go to **System Management > System Settings > System > Notification**.

Mail Server Settings

Mail Server IP Address/FQDN - Port

Specify Mail server IP address or FQDN and port number.

Authentication Required

If Enabled, specify authentication parameters i.e. username and password.

Figure 37: Mail Server Settings

Email Settings

From Email Address

Specify the email address from which the notification is to be mailed.

Send Notification to Email Address

Specify the email address to which the notification should be mailed.

| | |
|---------------------------------------|----------------------|
| From Email Address * | <input type="text"/> |
| Send Notifications to Email Address * | <input type="text"/> |

Figure 38: Email Settings

Time

Device's current date and time can be set according to the device's internal clock or synchronized with an NTP server. Device clock can be tuned to show the right time using global time servers so that logs show the precise time and the device's internal activities can also happen at a precise time.

To configure time settings, go to **System Management > System Settings > System > Time**.

Current Time

Current system time.

Time Zone

Select time zone according to the geographical region in which the device is deployed.

Set Date & Time

Select to set device's date and time.

Date

Set the date of device's internal clock.

Time

Set the time of device's internal clock.

Sync with NTP server

Select if you want device to synchronize automatically its time with an NTP server.

Use pre-defined

Use the pre-defined NTP servers - asia.pool.ntp.org & in. pool.ntp.org or specify NTP server IP address or domain name to synchronize time with a specific NTP server.

Use Custom

If custom NTP server is defined, time will be synchronized with custom server and not the pre-defined servers.

Firewall Manager uses NTP Version 3 (RFC 1305). One can configure up to 10 NTP servers. At the time of synchronization, it queries each configured NTP server sequentially. When the query to the first server is not successful, device queries second server and so on until it gets a valid reply from one of the NTP servers configured.

Sync Status

Click on 'Sync Now' Button to synchronize device clock with the NTP Server.

Current Time: 2016-11-21 10:23:08

Time Zone: Europe/London

Use pre-defined NTP Server

Use Custom NTP Server (Enter NTP Server IP Address/Domain)

Search / Add +

Sync Now

Do not use NTP Server

Date: 11/21/2016

Time: 10 HH 23 MM 8 SS

Figure 39: Title

High Availability (HA)

Hardware failure such as a failure of the power supply, hard disk, or processor is the main reason behind the failure of Internet security system and/or a firewall. To provide reliable and continuous connection to the Internet and to provide central management, two devices can be configured to function as a single device and provide HA.

Clustering Technology is used to ensure HA. In a cluster, two devices are grouped together and instructed to work as single entity.

This section covers the following topics:

- [HA terminology](#)
- [Configuring HA](#)

How Cluster works

Device offers high availability by using Virtual MAC Address shared between a Primary device and an Auxiliary device linked together as a “cluster”.

Primary and Auxiliary device are physically connected over a dedicated HA link port.

Typically, traffic enters your network by passing through a network switch but in HA one of the devices in the cluster has a Virtual MAC Address and traffic is forwarded to the device which has the virtual MAC Address.

The device which has virtual MAC Address is the Primary device and other peer is Auxiliary device. Primary device acts as a load balancer and forwards the traffic to the Auxiliary device for processing. Auxiliary device can process traffic only if cluster is operating in the Active-Active mode.

If configured in Active-Passive mode, Primary device processes the entire traffic while Auxiliary device waits in a ready mode to operate as the Primary device, in case Primary device or any of the monitored links fail.

Auxiliary device monitors the Primary device through the dedicated HA link and if it does not receive any communication within the pre-configured time, the Primary device is considered to have failed. In this case, Auxiliary device takes ownership of the virtual MAC Address from Primary device and acts as temporarily as Primary device. Once Primary device is up it automatically takes over from the Auxiliary device.

The device from which HA is enabled goes in Standalone state while the other device rebooted. Once the other device comes up, synchronization process starts. It synchronizes time zone, signatures (Anti Virus, Web Categorization, IPS

and Application), database configurations (Firewall Manager and Managed devices), backups (Firewall Manager and Managed devices) and logs (Managed devices).

After a successful synchronization, the two Firewall Manager devices come into Primary – Auxiliary state. In this state every event which takes place on Primary device gets reflected in Auxiliary device immediately.

When the Primary device goes down an automatic Failover takes place and the Auxiliary device goes into Standalone state. This process may take 10 to 15 seconds depending on size of data. During this transition period the administrator may lose access to Firewall Manager HA cluster for a while.

HA terminology

1. HA Cluster

Group of two devices instructed to work as a single entity. Every HA Cluster has one Primary device and one Auxiliary device. The Primary device controls how the cluster operates. The roles that the Primary and Auxiliary devices play in the cluster depend on the configuration mode.

2. HA Configuration Modes

Active-Active

A configuration of HA cluster consists of a Primary device and one Auxiliary device. In this mode, both Primary device and Auxiliary device process traffic while primary unit is in charge of balancing the traffic. Decision of load balancing is taken by the Primary device. Auxiliary device can take over only in case of a primary unit failure. (Currently Firewall Manager can not be deployed in Active-Active HA mode).

Active-Passive

A configuration of HA cluster which consists of a Primary device and an Auxiliary device. In this mode, only the Primary device processes traffic while Auxiliary device remains in stand-by mode, ready to take over if a Primary device failure occurs.

3. Primary device

The Primary device also tracks the status of all cluster devices. In an Active-Active cluster, the Primary device receives entire network traffic and acts as the load balancer to redirect traffic to Auxiliary device.

In an Active-Passive cluster, the Primary device processes the network traffic while Auxiliary device does not process any traffic but remains ready to take over if Primary device fails.

4. Auxiliary device

Auxiliary device is always waits to become the Primary device.

In an active-active cluster, Auxiliary device processes the network traffic assigned to it by the Primary device. In case Primary device fails, Auxiliary device becomes the Primary device. In an active-passive cluster, Auxiliary device does not process network traffic and is in stand-by. It becomes active only when Primary device is not available to process the traffic.

5. Dedicated HA Link Port

Dedicated HA link is a direct physical link between the devices participating in HA cluster.

6. Load Balancing

An ability of HA cluster of balancing the traffic between nodes in the HA cluster.

7. Monitored Interface

Set of interfaces that are selected to be monitored. Each device monitors its own such interface and if any of them is goes down, device will remove itself from the cluster and failover occurs.

8. Virtual MAC

It is a MAC Address associated with the HA cluster. This address is sent in response when any of the machines make an ARP request to HA cluster. It is not the actual MAC Address and is not assigned to any interface of any unit in the cluster.

A Primary device owns the MAC Address and is used for routing network traffic. All external clients use this address to communicate with the HA cluster. In case of failover, new Primary device will have the same MAC Address as the failed Primary device. The cluster device which has a Virtual MAC Address acts as a Primary device.

9. Primary State

In Active-Active mode, the device that is in charge of receiving all the traffic and load balancing is said to be in "Primary" state. An device can be in "Primary" state only when the other device is in "Auxiliary" state.

In Active-Passive mode, the device in charge of processing all the traffic is said to be in the "Primary" state. An device can be in "Primary" state only when the other device is in "Auxiliary" state.

10. Auxiliary State

In Active-Active mode, the device that receives the traffic to be processed by it from the Primary device is called to be in "Auxiliary" state. An device can be in "Auxiliary" state only when the other device is in "Primary" state

In Active-Passive mode, the device which is not processing the traffic is called to be in "Auxiliary" state. An device can be in "Auxiliary" state only when the other device is in "Primary" state.

11. Standalone State

An device is called to be in Standalone state when it can still process network traffic and when the other device is not in position to process network traffic (i.e. in "Fault" state or shut down).

12. Fault State

An device is in fault state when it cannot process network traffic if a device or link fails.

13. Peer

Once the HA cluster is configured, cluster devices are termed as Peers i.e. for Primary device, Auxiliary device is its peer device and vice versa.

14. Synchronization

The process of sharing the various cluster configuration, between Cluster devices (HA peers). Reports generated are not synchronized.

15. Device failover

If an device does not receive any communication within the predetermined period of time from the HA peer, the peer device is considered to have failed. This process is termed as Device Failover as when this occurs, the peer device is taken over.

16. Link Failover

Both the device in an HA cluster continuously monitor the dedicated HA link and the interfaces configured to be monitored. If any of them fails it is called link failure.

17. Session failover

Whether it is a device or link failover, session failover occurs for forwarded TCP traffic except for the virus scanned sessions that are in progress, VPN sessions, UDP, ICMP, multicast, and broadcast sessions and Proxy traffic.

Device normally maintains session information for TCP traffic which is not passing through proxy service. Hence, in case of failover, the device which takes over will take care of all the sessions (TCP session not passing through proxy application). The entire process is transparent for the end users.

Configure HA

Use to

- [Configuring Primary/Auxiliary Devices](#)
- [Disable HA](#)

Points to be noted

Behavior

- HA can be disabled from Primary device only which results into disabling HA on both the devices.
- After disabling HA, Primary device IP schema will not change.
- After disabling HA, Auxillary device will reboot with Factory Default settings (if connected).
- All administrators can login to auxillary device but the device will be accessible as read-only.
- Make sure that the IP Address of HA link port of Primary and Auxiliary devices are in same subnet.
- Disabling HA is required to restore backup.

Before configuring HA

Before attempting to configure two devices as an HA pair for Hardware Failover, check the following requirements:

- Both devices in the HA cluster i.e. Primary and Auxiliary device must be registered and have same number of interfaces. Both the member devices should be of the same model.
- Both devices in the HA cluster must have the same version installed on it.
- Two separate licenses are required, one for the Primary device and other for the Auxiliary device.
- Cables to all the monitored ports on both the devices must be connected. Connect dedicated HA link port of both the devices with crossover cable.
- Dedicated HA link port should have a unique IP Address on both the devices. SSH should be enabled for both the devices on DMZ Zone.

Configuring Primary/Auxiliary Devices

Use this page to configure the Primary/Auxiliary device.



Note:

- No changes in the firewall configuration. Only need to enable SSH on the dedicated interface.
- Allow SSH traffic for dedicated HA link port on both the devices through Device Access.

1. Go to **System Management > System Settings > System > HA**.
2. Enter High Availability details.

Serial Number

Displays Serial Number of Device.

Peer Serial Number

Displays peer's Serial Number if HA is enabled.

In case of Primary Device, it displays the Auxiliary Serial Number.

In case of Auxiliary Device, it displays the Primary Serial Number.

Initial HA Device State

Select to set intital device state from the available options.

Available Options:

- Primary
- Auxiliary

Passphrase

Passphrase - Specify a passphrase for communication.

Confirm Passphrase - Confirm the specified passphrase.



Note: To configure HA, both devices in the cluster must have the same passphrase.

Dedicated HA Link Port


Specify HA link port.

HA peers are physically connected using a crossover cable through this port. The same port must be used as an HA link port on peer Device also.

For example, if port E is configured as HA link port on Primary Device then use port E only as HA link port on Auxiliary Device. Make sure that the IP Address of HA link port for both, the Primary Device and Auxiliary Devices are in same subnet and SSH is enabled on both. Cluster Devices use this link to communicate cluster information and to synchronize with each other.


Peer HA link IP

Specify IP Address configured on the HA link port of the peer Device.

 **Note:** Available only for Primary Device.

Peer Administration Port


Specify Administration Port for Auxiliary Device. This port can be used for administration purpose.

 **Note:** Available only for Primary Device.

Peer Administration IP

Specify Administration IP Address for Auxiliary Device.


With this IP Address, the Admin Console of Auxiliary Device can be accessed. Any user accessing Web Admin Console of Auxiliary Device will be logged -in with HA Profile and have read-only rights.


 **Note:** Available only for Primary Device.

Select Ports to be Monitored


Select the ports to be monitored.


Both the Devices will monitor their own ports and if any of the monitored port goes down, Device will leave the cluster and failover will occur.


 **Note:** This feature is not supported in Virtual Security Devices.

 **Note:** Available only for Primary Device.

3. Click **Enable HA** to enable HA.

 **Note:** The Device from which HA is enabled, acts as a primary Device while the peer Device acts as auxiliary Device.

 **Note:** This feature is not supported in Virtual Security Devices.

 **Note:** Available only for Primary Device.

| Serial Number | M720224H9WG97C0 | | | | | | | | | | | | |
|--------------------------------|--|-----------|---------------|-------------------|--|--------------------------------|--|--------------------------------|--|--------------------------------|--|--------------------------------|--|
| Peer Serial Number | - | | | | | | | | | | | | |
| Initial HA Device State * | Primary ▼ | | | | | | | | | | | | |
| Passphrase * | Passphrase | | | | | | | | | | | | |
| | Confirm Passphrase | | | | | | | | | | | | |
| Dedicated HA Link Port * | Port1 ▼ | | | | | | | | | | | | |
| Peer HA link IP * | | | | | | | | | | | | | |
| Peer Administration Port * | Port2 ▼ | | | | | | | | | | | | |
| Peer Administration IP * | | | | | | | | | | | | | |
| Select Ports to be Monitored | <table border="1"> <thead> <tr> <th>Port List</th> <th>Selected Port</th> </tr> </thead> <tbody> <tr> <td>type to search...</td> <td></td> </tr> <tr> <td><input type="checkbox"/> Port1</td> <td></td> </tr> <tr> <td><input type="checkbox"/> Port2</td> <td></td> </tr> <tr> <td><input type="checkbox"/> Port3</td> <td></td> </tr> <tr> <td><input type="checkbox"/> Port4</td> <td></td> </tr> </tbody> </table> | Port List | Selected Port | type to search... | | <input type="checkbox"/> Port1 | | <input type="checkbox"/> Port2 | | <input type="checkbox"/> Port3 | | <input type="checkbox"/> Port4 | |
| Port List | Selected Port | | | | | | | | | | | | |
| type to search... | | | | | | | | | | | | | |
| <input type="checkbox"/> Port1 | | | | | | | | | | | | | |
| <input type="checkbox"/> Port2 | | | | | | | | | | | | | |
| <input type="checkbox"/> Port3 | | | | | | | | | | | | | |
| <input type="checkbox"/> Port4 | | | | | | | | | | | | | |

Figure 40: High Availability Details

If everything is cabled and configured properly and HA is enabled successfully:

- Both Devices will have the same configuration except the HA link port IP Address.
- By default, as soon as HA is enabled successfully, both the Devices will synchronize automatically.

Disable HA

HA can be disabled from this page.

Go to **System Management > System > System Services > HA** and click **Disable HA**

Network

Use **Network** pages to configure Firewall Manager Device to operate in your network.

This section covers the following topics:

- [Interface](#) - Configure and manage the ports/interfaces of the device.
- [DNS](#)- Manage DNS servers to be used by the Device, DNS Host Entries and routing of specific requests.
- [WAN Link Manager](#)- Manage device's WAN Link.
- [Unicast Route](#) - Allows to manage unicast routes.

Interface

Use **Interface** page to view port wise network (physical interface) and zone details. Alias details is nested and displayed beneath the respective physical interface, if configured.

To manage interfaces, go to **System Management > System Settings > Network > Interface**.

Add Alias

Alias allows binding multiple IP addresses onto a single physical interface. It is another name of the interface that will easily distinguish this interface from another.

1. Go to **System Management > System Settings > Network > Interface** and select **Add Alias**.
2. Enter alias details.

Physical Interface

Select Physical Interface for which Alias is to be bounded.

IP Family

Select IP family to add an alias.

Available Options:IPv4IPv6

Alias

Select type of IP address to be assigned to Alias.

Available Options:SingleRange

IP Address

Specify IP Address.

Netmask


Select the network subnet mask.

Figure 41: Add Alias

3. Select **Save**.

Edit Interface

This page allows you to change IP address and sub netmask of the Interface and gateway (if defined).

1. Go to **System Management > System Settings > Network > Interface** and click on the manage icon  under the Manage tab.
2. Enter general settings details.

Physical Interface

Physical Interface for example, Port A, Port B and so on. It cannot be modified.



Note: For the following SFM models, port names will be displayed as alphanumeric characters (for example, Port 1, Port 2 and so on) instead of alphabetic characters:

- SFM200
- SFM300
- SFM400

IPv4/Netmask

Specify IP Address and Netmask for the IPv4 Interface.

IPv6/Prefix

Specify IP Address and Prefix for the IPv6 Interface.

Gateway Name

Specify name of the gateway (It is available only when the gateway is defined on the interface)

IP Address

Specify IP Address of the gateway.

IPv6 Address (Available if IPv6 Configuration is enabled)

Specify IPv6 Address of the gateway.

3. Enter advanced setting details.

Interface Speed

Select Interface speed for synchronization.

Speed mismatch between Firewall Manager and 3rd party routers and switches can result into errors or collisions on interface, no connection, traffic latency or slow performance.

Available Options: Auto Negotiate 10 Mbps - Full duplex 10 Mbps - Half duplex 100 Mbps - Full duplex 100 Mbps - Half duplex 1000 Mbps - Full duplex 1000 Mbps - Half duplex

Default - Auto Negotiate

MTU

Specify MTU value (Maximum Transmission Unit)

MTU is the largest physical packet size, in bytes, that a network can transmit. This parameter becomes an issue when networks are interconnected and the networks have different MTU sizes.

Any packets larger than the MTU value are divided (fragmented) into smaller packets before being sent.

Default - 1500

Input range - 576 to 1500

4. Select Save.

DNS

The Domain Name System (DNS) is a system that provides a method for identifying hosts on the Internet using alphanumeric names called fully qualified domain names (FQDNs) instead of using difficult to remember numeric IP addresses. In other words, it translates domain names to IP addresses and vice versa.

DNS server is configured at the time of deployment. You can add additional IP addresses of the DNS servers to which device can connect for name resolution. When multiple DNS are configured, they are queried in the order as they are entered.

To configure DNS, go to **System Management > System Settings > Network > DNS**.

DNS List IPv4

Specify the DNS IP Address based on priority in DNS 1, DNS 2 and/or DNS 3.

| IPv4 | |
|-------|--------------------------------------|
| DNS 1 | <input type="text" value="8.8.8.8"/> |
| DNS 2 | <input type="text" value="4.2.2.2"/> |
| DNS 3 | <input type="text" value="4.4.4.4"/> |

Figure 42: DNS List



Note: Do not forget to click **Apply** after adding new IP address to the DNS list.


WAN Link Manager

WAN Link routes traffic between the networks. By default, Firewall Manager supports only one WAN Link. You must have configured the IP address for a default WAN Link at the time of deployment. You can change this configuration any time if required.

To configure WAN Link, go to **System Management > System Settings > Network > WAN Link Manager**

Edit WAN Link

This page allows you to edit the WAN Link.

1. Go to **System Management > System Settings > Network > WAN Link Manager**
2. Select the Gateway which you want to edit by clicking the Manage icon  in the Manage column.
3. Modify the gateway details.

Name

Gateway Name

IPv4 Address

Specify IP Address

IPv6 Address

Specify IPv6 Address

Interface

Specify Ethernet Port number that is to act as a Gateway.

| | |
|----------------|---|
| Name * | Default Gateway |
| IPv4 Address * | <input type="text" value="10.198.45.10"/> |
| IPv6 Address | <input type="text" value="Enter IPv6 Address"/> |
| Interface * | <input type="text" value="PortA"/> ▼ |

Figure 43: Gateway Detail

4. Select **Save**.

Unicast Route

This page allows you to manage unicast routes. To configure unicast static routes, define the destination IP address and netmask of packets that the device is intended to intercept, and provide a (gateway or next hop) IP address for those packets. The gateway address specifies the next-hop router to which traffic will be routed. Also, provide the interface and the approximate distance for routing.

To manage unicast routes, go to **System Management > System Settings > Network > Unicast Route**.

Add Unicast Route

This page allows you to configure Unicast Route.

1. For IPv4 Unicast Route, navigate to **System Management > System Settings > Network > Unicast Route** and click **Add** under IPv4 Unicast Route. For IPv6 Unicast Route, navigate to **System Management > System Settings > Network > Unicast Route** and click **Add** under IPv6 Unicast Route.
2. Enter the details.

Destination IP/Prefix

Specify Destination IP Address and prefix.

Gateway

Specify Gateway IP Address.

Interface

Select Interface from the list.

Distance

Specify Distance for routing. Range of value is from 0 to 255.

| | | | |
|-----------------------------|---|-----------|--|
| Destination IP * / Prefix * | <input type="text" value=" "/> | / | <input type="text" value="/32 (255.255.255.255)"/> |
| Gateway * | <input type="text"/> | | |
| Interface | <input type="text" value="Select Interface"/> | | |
| Distance | <input type="text" value="0"/> | (0 - 255) | |

Figure 44: Add Unicast Route (IPv4)

| | | | |
|-----------------------------|---|-----------|----------------------|
| Destination IP * / Prefix * | <input type="text" value=" "/> | / | <input type="text"/> |
| Gateway * | <input type="text"/> | | |
| Interface | <input type="text" value="Select Interface"/> | | |
| Distance | <input type="text" value="0"/> | (0 - 255) | |

Figure 45: Add Unicast Route (IPv6)

3. Click **Save**.

Maintenance

Maintenance facilitates handling the maintenance of the managed devices.

Using the Maintenance menu, you can configure following operation:

- *Backup & Restore*- Allows to manually take backup or schedule backup of the managed devices.
- *Compatibility Management* - Allows you get the compatibility information or acquire compatibility of upcoming OS versions.
- *Inactive Users Maintenance* - Allows you to get report on the inactive users, also to delete the inactive users.

Backup & Restore

Backup is the essential part of data protection. Backups are necessary in order to recover data from the loss due to the disk failure, accidental deletion or file corruption. There are many ways of taking backup and just as many types of media to use as well.

The Backup and Restore menu enables you to back up and restore your Firewall Manager. It is a good idea to backup the Firewall Manager configuration on a regular basis to ensure that, should the system fail, you can quickly get the system back to its original state with minimal effect to the network. It is a good idea to back up the configuration after making any changes to the configuration of the Firewall Manager or settings that affect the managed devices.

Once the backup is taken, you need to upload the file for restoring the backup. Restoring data older than the current data will lead to the loss of current data.

Administrator can schedule Firewall Manager backup or manually take the backup from **System Management > System Settings > Maintenance > Backup & Restore**.

Backup Restore

To take the backup manually and restore, go to **System Management > System Settings > Maintenance > Backup & Restore** and click **Backup Now** and then select the backup to be restored and click **Upload and Restore**. Alternatively use the **Browse** button to select the complete path.



The screenshot shows a web interface with two main sections. The top section is titled "Backup Configuration" and contains a button labeled "Backup Now". The bottom section is titled "Restore Configuration" and contains a button labeled "Choose File" followed by the text "No file chosen".

Figure 46: Backup Restore



Note: Sophos Firewall Manager Password will not be restored during this process.

Schedule Backup

Backup Frequency

Select backup frequency.

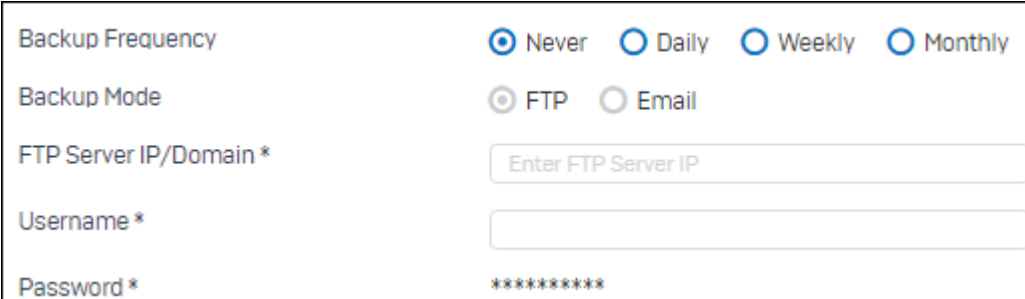
In general, it is best to schedule backup on regular basis. Depending on how much information you add or change will help you determine the schedule.

Available Options: **Never** - Select this option if you do not want to take backup. **Daily** - Configure time at which the backup should be taken. **Weekly** - Configure day and time at which the backup should be taken. **Monthly** - Configure day and time at which the backup should be taken.

Backup Mode

Select how and to whom backup files should be sent.

Available Options: **FTP** - If backup is to be stored on FTP server, configure **FTP server IP/Domain** address, username and password to be used. **Mail** - If backup is to be mailed, specify **Email Address** on which backup is to be mailed.



The screenshot shows a configuration form for scheduling backups. It includes the following fields and options:

- Backup Frequency:** Radio buttons for **Never** (selected), **Daily**, **Weekly**, and **Monthly**.
- Backup Mode:** Radio buttons for **FTP** (selected) and **Email**.
- FTP Server IP/Domain *:** A text input field with the placeholder text "Enter FTP Server IP".
- Username *:** A text input field.
- Password *:** A text input field with masked characters (*****).

Figure 47: Schedule Backup

Manage Backup


This section displays the list of last five backups along with the time and size of the backup. It also provides an option to download the backup and restore it.

Firmware

System > Maintenance > Firmware

Firmware

Firmware page displays the list of available firmware versions downloaded. Maximum two firmware versions are available simultaneously and one of the two firmware versions is active.

Upload firmware  - Administrator can upload a new firmware. Click to specify the location of the firmware image or browse to locate the file. You can simply upload the image or upload and boot from the image. The uploaded firmware can only be active after the next reboot.


In case of Upload & Boot, firmware image is uploaded and upgraded to the new version, closes all sessions, restarts, and displays the login page. This process may take few minutes since the entire configuration is also migrated in this process.

Boot from firmware  - Option to boot from the downloaded image and activate the respective firmware.

Boot with factory default configuration  - Device is rebooted and loads default configuration.



Note: Entire configuration will be lost if this option is selected.

Active  - Active icon against a firmware suggests that the device is using that firmware.

Available Latest Firmware

Check For New Firmware

Displays if any new firmware is available.

Firmware Version

List of available firmware versions that can be downloaded.

Type

Different types of firmware.

Available Options:BetaGA

Actions

Download Button to download the firmware. Once the firmware is downloaded, click the **Install** button to install the firmware.

SFOS Hotfix

Allow auto-install of important Hot-fixes

Hotfixes are applied automatically if available. Disable if you do not want to apply hotfix.

Default - Enable

Licensing

This page displays Firewall Manager device's registration information.

Device Registration Details

Model

Firewall Manager device model number.

Version

Firewall Manager firmware version number.

Company Name

Name of the company under whose name the device is registered.

Contact Person

Name of the contact person from the company.

Registered Email ID

Email address used at the time of device registration.

Module Subscription Details

Enhanced Support

Subscription status and Expiry Date (if the module is subscribed).

Possible status:SubscribedUnsubscribedExpiredEvaluating

Enhanced Plus Support

Subscription status and Expiry Date (if the module is subscribed).

Possible status:SubscribedUnsubscribedExpiredEvaluating

Manage Subscription Online

Displays alert message if the Firewall Manager device is not registered.

Synchronize Device Licenses

Click to synchronize device licenses with Customer My Account.

Link to Customer My Account to register device or to update and renew subscription modules.

Activate Subscription

Click to avail subscriptions e.g. support using the **Subscription Key**.

Activate Subscription

This page allows you to enter Subscription Key for SFM.

1. Go to **System Management > System Settings > Maintenance > Licensing** and click on **Activate** under **Manage Subscription Online** section.
2. Enter the **Subscription Key** and click **Verify** to verify the key.

Content Distribution

Content Distribution page is used to manage or view the status of various pattern updates for security services. To manage content distribution, go to **System Management > System Settings > Content Distribution**.

Updates Status

Pattern

Displays the pattern type. Available types are:

- AP Firmware
- ATP
- Authentication Clients
- Avira AV
- IPS
- RED Firmware
- Sophos AV
- SSLVPN Clients
- WAF

Model

Displays the model of the SF device for which the pattern is applicable.

Version

Displays version of the pattern.

Update Type

Displays update type for the pattern. Available types are:

- Full Upgrade - Shows that the upgrade is to the latest version of the pattern.
- Upgrade to next version - Shows that the upgrade is to the immediate next version of the pattern.
- Incremental Upgrade from (base version) to (incremental version) - Shows that the upgrade is from a base version to an incremental version of the pattern.

Example: Suppose Version A, Version B, Version C and Version D are various versions of a pattern in sequence, then following is applicable for various **Update Types**:

- If upgrade is from Version A to Version B then that update is categorized as **Upgrade to next version**.
- If upgrade is from Version A to Version C then that update is categorized as **Incremental Upgrade from Version A to Version C**.
- If upgrade is from Version A to Version D then that update is categorized as **Full Upgrade**.

Last Successful Download

Displays the time of last successful download in HH:MM:SS, Mon DD YYYY format.

Update Pattern Now

Click to update available patterns.

Pattern download/installation

Auto Update

Click to enable automatic updates for patterns.

Interval

Select the frequency of the updates. Available options are:

- Every hour
- Every 2 hours
- Every 4 hours
- Every 12 hours
- Daily
- Every 2 days

Apply

Click to save settings.

Diagnostics

Diagnostic page allows checking the health of your Firewall Manager device in a single shot. Information can be used for troubleshooting and diagnosing problems found in your Firewall Manager device.

It is like a periodic health checkup that helps to identify the impending device related problems. After identifying the problem, appropriate actions can be taken to solve the problems and keep the device running smoothly and efficiently.

This section covers the following topics:

- [Tools](#) - Provides diagnostic tools to test and troubleshoot network issues.
- [Troubleshoot Report](#) - Use to generate Consolidated Troubleshooting Report.
- [System Graph](#) - View CPU and Memory usage of Firewall Manager device of last two hours.

Tools

This page provides diagnostic tools to test and troubleshoot network issues such as packet loss, connectivity errors or discrepancies in the Firewall Manager network.

Go to **System Management > System Settings > Diagnostics > Tools** to view the various statistics.

- Ping
- Trace route
- Name lookup
- Route lookup

Ping

Ping is a most common network administration utility used to test the reachability of a host on an Internet Protocol (IP) network and to measure the round-trip time for messages sent from the originating host to a destination computer.

Ping sends ICMP echo request/replies to test connectivity to other hosts. Use standard ICMP ping to confirm that the server is responding. Ping confirms that the server can respond to an ICMP ping request.

Use Ping diagnostically to:

- Ensure that a host computer you are trying to reach is actually operating or address is reachable or not
- Check how long it takes to get a response back
- Get the IP address from the domain name
- Check for the packet loss

IP Address/Host Name

IP Address or fully qualified domain name to be pinged.

It determines network connection between Firewall Manager and host on the network. The output shows if the response was received, packets transmitted and received, packet loss if any and the round-trip time. If a host is not responding, ping displays 100% packet loss.

Interface

Interface through which the ICMP echo requests are to be sent.

Size

Ping packet size

Range - 1 to 65507

Trace Route

Trace Route is a useful tool to determine if a packet or communications stream is being stopped at the Firewall Manager, or is lost on the Internet by tracing the path taken by a packet from the source system to the destination system, over the Internet.

Use traceroute to:

- find any discrepancies in the Firewall Manager network or the ISP network within milliseconds
- trace the path taken by a packet from the source system to the destination system, over the Internet

IP Address/Host Name

IP Address or fully qualified domain name.

It determines network connection between Firewall Manager and host on the network. The output shows all the routers through which data packets pass on way to the destination system from the source system, maximum hops and Total time taken by the packet to return measured in milliseconds.

Interface

Interface through which the requests are to be sent.

Name Lookup

Name lookup is used to query the Domain Name Service for information about domain names and IP addresses. It sends a domain name query packet to a configured domain name system (DNS) server. If you enter a domain name, you get back the IP address to which it corresponds, and if you enter an IP address, then you get back the domain name to which it corresponds. In other words, it reaches out over the Internet to do a DNS lookup from an authorized name server, and displays the information in the user understandable format.

IP Address/Host Name

IP address or fully qualified domain name that needs to be resolved.

DNS Server IP

DNS server to which the query is to be sent.

Route Lookup

If you have routable networks and wish to search through which Interface Firewall Manager routes the traffic then lookup the route for the IP address.

IP Address

IP address that needs to be resolved.

Troubleshoot Report

To help Support team to debug the system problems, troubleshooting report can be generated which consists of the system's current status file and log files. File contains details like list of all the processes currently running on system, resource usage etc. in the encrypted form.

Customer has to generate and mail the saved file at support@SF.com for diagnosing and troubleshooting the issue. File will be generated with the name: _TSR_<APPKEY>_<MM_DD_YY >

Where, APPKEY is the device key of the device for which the report is generated and MM_DD_YY is the date (month date year) on which the report is generated.

Go to **System Management > System Settings > Diagnostics > Troubleshoot Report** to generate Consolidated Troubleshooting Report (TSR).

Enter Consolidating Troubleshooting Report details:

Generate Troubleshoot Report for

Select components for which troubleshoot report has to be generated.

Available Options:System SnapshotLog Files

Reason

Specify reason to generate troubleshoot report.

Generate Button

Click to generate troubleshoot report.

System Graph

Use System Graph page to view CPU and Memory usage of Firewall Manager device for last two hours. The usage is displayed in the form of graphs.

Go to **System Management > System Settings > Diagnostics > System Graph** to view the CPU and memory usage.

Appendix A - Compatibility with SFOS

| | | SFOS v16 | SFOS v16.5 (till MR-5) |
|----------------------|-------------------|-----------|---|
| SF MOS V16.05 GA | Device Mgmt. | Supported | Supported |
| | Group Level Mgmt. | Supported | Supported (except new SFOS features post v 16.5 GA) |
| | Template Mgmt. | Supported | Supported |
| | Firmware Upgrade | Supported | Supported |
| SF MOS V16.01.1 RC-1 | Device Mgmt. | Supported | Supported |
| | Group Level Mgmt. | Supported | Supported (except new SFOS features) |

| | | |
|-------------------------|--|--|
| Template Mgmt. | Import: Supported till SFOS 16.1 MR-1 Export: Supported | Import: Not Supported Export: Supported |
| Firmware Upgrade | Supported | Supported |

Copyright Notice

Copyright 2016-2017 Sophos Limited. All rights reserved.

Sophos is a registered trademark of Sophos Limited and Sophos Group. All other product and company names mentioned are trademarks or registered trademarks of their respective owners.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise unless you are either a valid licensee where the documentation can be reproduced in accordance with the license terms or you otherwise have the prior permission in writing of the copyright owner.