# Contents

**Introduction** ................................................................................................................................... 3

**Using Admin Console** .................................................................................................................. 4
  Supported Browsers.......................................................................................................................... 5
  Navigating through the Admin Console........................................................................................... 5
  Menus............................................................................................................................................... 6
  Tool Tips.......................................................................................................................................... 6
  Notification pop-ups......................................................................................................................... 7
  Common Operations.......................................................................................................................... 7
  Set Schedule.................................................................................................................................. 7
  Synchronize.................................................................................................................................... 8
  Entity Usage Reference...................................................................................................................... 8
  Editing an Entity............................................................................................................................... 8
  Deleting an Entity............................................................................................................................ 8
  Sorting Lists................................................................................................................................... 9
  Filtering Lists.................................................................................................................................. 9
  Configuring Column Settings......................................................................................................... 9
  Reordering Lists.............................................................................................................................. 9
  Summary......................................................................................................................................... 9

**Templates** ................................................................................................................................... 9

**System & Monitor** ....................................................................................................................... 10
  Device Settings............................................................................................................................... 10
  Managed Devices............................................................................................................................ 10
  Maintenance.................................................................................................................................... 24
  Firmware......................................................................................................................................... 26
  Scheduled Task............................................................................................................................... 27
  Dynamic Objects............................................................................................................................ 27
  Change Control............................................................................................................................... 32
  Monitor.......................................................................................................................................... 37
  Device Monitor............................................................................................................................... 37
  Graphs............................................................................................................................................ 39
  Alerts............................................................................................................................................. 41
  Event Viewer................................................................................................................................. 43
  Account Settings............................................................................................................................ 44
  Accounts......................................................................................................................................... 44
  Administration................................................................................................................................. 46
  Diagnostics.................................................................................................................................... 50

**Copyright Notice** ....................................................................................................................... 52
Introduction

Sophos Central Firewall Manager (CFM) provides comprehensive central management of Sophos XG Firewalls to Sophos Partners. With a range of features, CFM 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.

The Sophos Central Firewall Manager UI offers you 3 work areas: Device Configuration, Templates, and System & Monitor.

Device Configuration

The Device Configuration work area allows you to manage policies and configurations of individual or group of Sophos XG 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.

Templates

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 & Monitor

The System & Monitor work area lets you manage device settings, monitoring settings and your CFM 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.
- Account Settings: You can manage CFM account settings, and set up role-based access, Diagnostics and more.

Dashboards & Monitoring

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

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 Web Address of the Sophos Central Firewall Manager in the browser’s URL box. A dialog box appears prompting you to enter email and password.

Below are the screen elements with their description:

Email
Enter registered Partner email address.

Password
Enter Partner account password.

Login button
Click to log on the Admin Console.

You will be redirected to Login Verification page. Enter Security Code and PIN to continue.

Below are the screen elements with their description:

Security Code
Enter Security Code as received on your registered Partner email address.

PIN
Enter PIN for your Partner account.

Submit
Click to submit entered information.

Choose Another Method
Click to select another method for login verification.

Home appears as soon as you press Submit on Login Verification page.

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 out procedure

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

You can connect to CFM 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 Central 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 CFM. 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 CFM.
• Discover – Click to view list of devices sending heartbeat packet to the CFM. 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.
• Language - Click to change language.
• Help – CFM 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.

**Menus**

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

![SOPHOS Central Firewall Manager](image)

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.

The left navigation bar expands and contracts dynamically when clicked on without navigating to a submenu. When you click on a top-level heading in the left navigation bar, 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.

**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.

![Success Notification]

![Error Notification]

**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 Account 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).

**Synchronize**

You can synchronize configuration of selected entities of managed device(s) with the configuration available in CFM. 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. CFM 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 & Monitor is meant to manage and configure the basic system options for the Sophos Central Firewall Manager. This includes the basic network settings to connect the Sophos Central Firewall Manager to the corporate network, the configuration of administrators and their access privileges, managing and updating firmware for the Sophos Central Firewall Manager, as well as managed Devices.

System allows you to configure the following settings:

- Device Settings
- Monitoring
- Account Settings

**Device Settings**

Device Settings menu enables the administrator to add devices to the Sophos Central 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 Sophos Central 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 Sophos Central Firewall Manager Sophos Central 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 Sophos Central Firewall Manager.

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

Select if the managed device is directly accessible from Sophos Central 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 Sophos Central 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 Sophos Central 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 Sophos Central 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 Sophos Central Firewall Manager and the managed device.

---

3. Click Save.
Add Device Wizard

The Add device wizard enables you to add a device, configure firmware, restore backup, and apply a template.

Wizard is divided into six sections:

1. Device
2. Users
3. Firmwares
4. Restore backup
5. Template
6. Summary

1. Go to System & monitor > Device settings > Managed devices > Device discovery and click 🔄. Alternatively, click Discover 🌟 to run the wizard.

2. Add device information
   a) Enter the Device name.
   b) Enter the Serial number. This field will be autopopulated if you run the wizard from Discover notification.
   c) Enter the IP/Domain assigned to the WAN interface of the Device.
   d) Enter the Firewall admin username.
   e) Enter the Password.
   f) Enter a Description.
   g) Click Enable change control (CCL).
   h) Click Administrator information to add more information of the firewall manager's administrator.
   i) Enter the Administrator name.
   j) Enter the Contact number.
   k) Enter the Email ID.
   l) Select the Communication mode.

Firewall manager will push configuration changes to the firewall

Select if the managed device is directly accessible from the firewall manager without an intermediate NAT box. Specify the access protocol and port number to communicate with the managed device.

Click to Test connection.

The device will fetch configuration changes from the firewall manager

Select if the managed device is behind a NAT box (Example: ADSL). The managed device will poll the firewall manager for configuration updates at one-minute intervals and pull the available updates.

m) Specify the port on which the device and firewall manager should communicate.

n) Click Next to go to Communication mode or Skip to finish to complete the wizard.
3. Select the firewall manager users.
   a) Add **Firewall manager users** to manage the device.
   b) Click **Back** to go to **Device** or **Next** to go to **Firmwares** or **Skip to finish** to complete the wizard.

4. Configure firmware settings
   Displays the current firmware version of managed devices, and availability of the latest firmware version.
   a) If the device model is available in the firewall manager, the latest version will appear automatically. If it doesn't, go to **System & monitor > Device settings > Firmware** and click **Check for latest firmwares**
   b) Click **Yes** to upgrade the device with the latest available firmware. It is disabled by default.
   c) Click **Back** to go to **Users** and **Next** to go to **Restore backup** or **Skip to finish** to complete the wizard.
Figure 4: Upgrade device firmware

5. Configure restore backup
   a) Click **Yes** to restore the backup of an existing device in the new device. It is disabled by default.
   b) Select an existing device and the backup you wish to restore in the new device. Alternatively, upload the backup file from your computer and restore it in the new device.
   c) Click **Back** to go to **Firmwares** or **Next** to go to **Template** or **Skip to finish** to complete the wizard.

Figure 5: Restore existing configuration backup

6. Configure template management
   a) Click **Yes** to apply an existing template to the device. The template is disabled by default.
   b) Select the template to be applied.
   c) Click **Next** to view **Summary** or **Back** to go to **Restore backup**. Click **Skip to finish** to complete the wizard.
Figure 6: Select the template to configure the device

7. Review configuration summary.

Summary displays details of the added device, including the device name, device key, IP/Domain, admin username, communication mode, communication ports of firewall manager and XG Firewall, and the status of firmware upgrade, restore backup, and template application.

Click **Finish** to complete the wizard or **Back** to go to **Template**.

Figure 7: Summary

**Export Device List**

Export Device List option is used to export the list of all managed devices added in the Sophos Central 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 the last 30 days.

This report is generated automatically at 11:50 PM Daily.

To download the report, follow the steps shown below.

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.

**All Managed Devices**

Displays list of all devices that are managed by Sophos Central Firewall Manager.

- **Device Name**: Displays name of the device.
- **Serial Number**: Displays Serial Number of the device.
- **Company Name**: Displays company Name for the device.
- **Model**: Displays Model Name for the device.
- **Status**: Displays Status for the device.

**Device Discovery**

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

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.

   ![Figure 8: Add Device Group](image)

   **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. CFM 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 Sophos Central 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.

![Figure 9: Add Template](image)

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.
- **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 Sophos Central Firewall Manager. Sophos Central Firewall Manager acts as a Backup repository for device backups. Administrator can restore this backup on the device whenever required. Sophos Central 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.
**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.
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.

![Figure 12: Inactive Users Report](image)

**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.

![Figure 13: Delete Inactive Users](image)

**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).

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 Sophos Central 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 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 refrential 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](image)

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.
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.

![Image of Zone Details](image)

**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.

![Image of Device-Zone Mapping](image)

**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: IPv4 IPv6
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 Manager 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**: IPv4 IPv6

   ![Figure 20: Add Gateway details](image)

3. Enter Device-Gateway Mapping details.

   **Device**
   Select the device.

   **Gateway**
   Select the gateway.

   ![Figure 21: Device-Gateway Mapping](image)

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 Sophos Central Firewall Manager and stored in Sophos Central 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 Sophos Central Firewall Manager and stored in Sophos Central 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, Sophos Central 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 Sophos Central 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

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 Sophos Central Firewall Manager itself.

Sophos Central Firewall Manager also provides email alerts for monitoring device in case Administrator cannot log on to Sophos Central 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 heath information of the managed devices in graphical manner.

Device Monitor

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

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

- Resource: CPU, Memory, Disk (Report) and Disk (Config).
- 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 pattern 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

Sophos Central Firewall Manager allows administrator to create and send email alerts to the specified email address(es) based on predefined criteria. Sophos Central 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

CFM 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 Status.

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(es) to send alert notification through email.
You need to configure email server from System Management > Account 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).

Type
You can specify a consolidated email for alerts of all devices managed by Sophos Firewall Manager or a separate email per alert per device.

Note: The email subject displays the firewall name and serial number, the SFM serial number, and the specified profile name of the alert.

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 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.
3. Click Save.

Alerts

Sophos Central 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 Logs

Device Logs page allows to view the logs for modules like Application Filter, Web Filter, Malware 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 & Monitor > Monitor > Event Viewer > Device Logs > and select module and Device and click Get Data.

Click Open PCAP to view packet capture. It will display the packet captures that are automatically filtered based on the values of the currently selected packet.

Click Download to export the logs in a CSV file. Hover over module icons for a detailed view.

Available Log Modules:

- System – System logs provide information about all the system-related logs, including the logs for VPN events.
- Web Filter – Web filter logs provide web surfing details like accessed/blocked sites, users trying to access the blocked websites etc. and the action taken by the device (Allowed or Blocked).
- Application Filter – Application filter logs provide details about applications to which access was denied by the device.
- Malware – Malware logs provide information about the viruses identified by the device.
- Email – Email logs provide information about the mail traffic processed by the device.
• Firewall – Firewall logs provide information about how much traffic passes through a particular firewall rule and through which interfaces.
• IPS – IPS logs provide information about the intrusion attempts detected/blocked by the device.
• Authentication – Authentication logs provide information about all the authentication logs including firewall, VPN and User Portal authentication.
• Admin – Admin logs provide information about administrator event and tasks.
• WAF – WAF logs provide information about HTTP/S requests and action taken on the same.
• Advanced Threat Protection - ATP logs provide information related to threats detected/blocked by the device.
• Security Heartbeat - Security Heartbeat logs provide information on Heartbeat connection and status.

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 CFM 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 Events – Provides information of the administrative events and task occurred at Sophos Central Firewall Manager.
• System Events – Provides information of the system events and tasks occurred at Sophos Central Firewall Manager.

Account Settings

Account Settings allows configuration and administration of CFM Device for secure and remote management. It also provides the basic Account Settings of the Web Admin console. Configuration of several non-network features, such as Service Network, Portal Communication, Device Inventory and Time Zone Settings can also be done through Account Settings.

• Accounts on page 44
• Administration on page 46
• Diagnostics on page 50

Accounts

Accounts section allows you to view list of companies (Distributors/Partners/Resellers) and manage their respective devices which are part of CFM service network. It also allows configuration and synchronization of Partner Portal with CFM.

• Synchronize on page 44
• Device Inventory on page 45
• Settings on page 45

Synchronize

This page allows you to synchronize updated information on Partner Portal with CFM.

The Partner can synchronize CFM with available updated information on Partner Portal and can override all current configurations by synchronizing all the devices available on Partner Portal.

Go to System Management > Account Settings > Accounts > Synchronize click Synchronize to synchronize CFM with Partner Portal.
**Device Inventory**
This page displays the list of devices which are available for management through CFM.

Use Device Inventory page to view and manage Sophos XG Firewall devices to CFM.

To view and manage devices navigate to **System Management > Account Settings > Accounts > Device Inventory**.

- **Serial Number**: Serial Number of the managed device.
- **Company Name**: Name of the company which owns the device.
- **Contact Person**: Name of the contact person from the company.
- **Contact Number**: Contact number of the contact person.

**Add Device**
Use this page to add devices to CFM.

1. Go to **System Management > Account Settings > Accounts > Device Inventory**.
2. Click on **+** to add a new device.
3. Add device Details:
   a) **Device Name**: Specify Device name to uniquely identify the device.
   b) **Serial Number**: Displays Serial Number of the device.
   c) **Admin Username**: Specify Administrator Username of the device.
   d) **Password and Confirm Password**: Password for the above mentioned Administrator Username of the device.
   e) **Communication Mode**: Specify communication mode to manage Firewall device from CFM.
   f) **Central Management will push updates to this Device**: Select if the managed Sophos XG Firewall device is directly accessible from CFM, i.e. there is no intermediate NAT box. Specify access protocol and port number to communicate with managed Firewall device.
   g) **This Device will fetch updates from Central Management**: Select if the managed Firewall device is behind NAT box.
   h) **Template**: Select configuration template which has to be applied on the device.
   i) **Access Protocol**: Specify Protocol that is to be used to access the device for pushing configuration and synchronizing that is. Protocol used to communicate with the device.
   j) **Access Port**: Specify Port through which device and CFM should communicate.
   k) **Access to User**: Specify CFM Administrator who can manage the Device.
   l) **Description**: Specify description for the device.
   m) **Administrator Information**: Click hyperlink to add additional information of CFM Administrator.
   n) **Administrator Name**: Specify name of the Administrator.
   o) **Contact Number**: Specify contact number of the Administrator.
   p) **Email ID**: Specify email ID of the Administrator.
   q) **Customer Information**: Click hyperlink to view information of the customer.
   r) **Company**: Name of the company.
   s) **Contact Person**: Name of the contact person.
   t) **Contact Number**: Displays contact number of the contact person.
   u) **Test Connection**: Click to test the connectivity between CFM and the managed device.
4. Click **Save**.

**Settings**
Use this page to update Time Zone Settings and Sophos Adaptive Learning settings for CFM.

**Time Zone Settings**: Select relevant time zone for CFM.
**Apply:** Select to apply changes.

**Sophos Adaptive Learning**

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

Configuration and usage data such as Device information (hardware version, vendor), Firmware version and license information (not the owner), Features in use (status, on / off, count, HA status, Central Management status), amount of configured objects (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**

Following Application usage and Threat data is gathered:

- Unclassified applications to improve and enlarge the network visibility and application control library.
- Data for IPS alerts, virus detected (also URL for which virus found), spam, ATP threats such as threat name, threat URL/IP, source IP, and applications used.

Default - Enable

**Administration**

**Administration** covers general configuration of Sophos Central 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.

**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 Sophos XG Firewall Device and CFM 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, CFM 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 > Account 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 > Account Settings > Administration > Access profile >** and click **Add**.
2. Enter Profile details.

**Profile Name**

Name to identify the profile. By default Sophos Central 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.
3. Click Save.

Users

Use the Users page to view users. It allows configuring administrator access to the Sophos XG Firewall 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 Sophos Central Firewall Manager device options.
To manage users, go to **System Management > Account Settings > Administration > Users >**.

You can view added users, **add new users** or edit or delete existing users.

**Add User**

1. Go to **System Management > Account 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 Sophos Central Firewall Manager will be able to assign or update device groups.
Figure 26: Add User

3. Click Save.

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 Sophos Central Firewall Manager.

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

Diagnostics

Diagnostic page allows checking the health of your Sophos Central Firewall Manager device in a single shot. Information can be used for troubleshooting and diagnosing problems found in your Sophos Central 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 Sophos Central 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 Sophos Central Firewall Manager network.
Go to **System Management** > **Account 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 Sophos Central 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 Sophos Central 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 Sophos Central 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 Sophos Central Firewall Manager and host on the network. The output shows all the routers through which data packets pass on way to the destination 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 Sophos Central Firewall Manager routes
the traffic then lookup the route for the IP address.

**IP Address**

IP address that needs to be resolved.

---

**Copyright Notice**

Copyright 2016-2018 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.