



# Sophos XG Firewall Web Interface Reference and Admin Guide v17

For Sophos Customers  
Document Date: October 2017

# Contents

<b>Introduction.....</b>	<b>7</b>
Flavors.....	7
Administrative Interfaces.....	7
Administrative Access.....	7
<b>Using Admin Console.....</b>	<b>8</b>
Supported Browsers.....	10
Menus.....	10
Pages.....	11
List Navigation Controls.....	11
<b>Monitor and Analyze.....</b>	<b>11</b>
Control Center.....	11
Current Activities.....	18
Live Users.....	18
Live Connections.....	19
Live Connections IPv6.....	21
View Live Connection Details.....	23
IPsec Connections.....	27
Remote Users.....	27
Diagnostics.....	28
Tools.....	28
System Graphs.....	31
URL Category Lookup.....	37
Packet Capture.....	37
Connection List.....	43
Support Access.....	47
<b>System.....</b>	<b>48</b>
Profiles.....	48
Schedule.....	48
Access Time.....	50
Surfing Quotas.....	53
Network Traffic Quota.....	56
Network Address Translation.....	60
Device Access.....	61
Hosts and Services.....	63
IP Host.....	64
IP Host Group.....	65
MAC Host.....	66
FQDN Host.....	67
FQDN Host Group.....	68
Country Group.....	68
Services.....	69
Service Group.....	70
Administration.....	71

Licensing.....	72
Device Access.....	73
Admin Settings.....	76
Central Management.....	79
Time.....	81
Notification Settings.....	82
SNMP.....	84
Netflow.....	86
Messages.....	86
Certificates.....	86
Certificates.....	86
Certificate Authorities.....	89
Certificate Revocation Lists.....	90
Backup & Firmware.....	90
Backup & Firmware.....	91
API.....	92
Import Export.....	94
Firmware.....	95
Pattern Updates.....	97
<b>Configure.....</b>	<b>99</b>
Network.....	99
Interfaces.....	99
Zones.....	128
WAN Link Manager.....	130
DNS.....	136
DHCP.....	141
IPv6 Router Advertisement.....	147
Cellular WAN.....	151
IP Tunnels.....	153
Neighbors (ARP-NDP).....	155
Dynamic DNS.....	158
Authentication.....	160
Servers.....	161
Services.....	170
Groups.....	178
Users.....	182
One-Time Password.....	189
Captive Portal.....	192
Guest Users.....	195
Clientless Users.....	201
Guest User Settings.....	204
Client Downloads.....	209
STAS.....	210
VPN.....	211
IPsec Connections.....	212
SSL VPN (Remote Access).....	219
SSL VPN (Site to Site).....	221
CISCO™ VPN Client.....	224
L2TP (Remote Access).....	227
Clientless Access.....	231
Bookmarks.....	231
Bookmark Groups.....	233
PPTP (Remote Access).....	233
<b>IPsec Profiles.....</b>	<b>235</b>

SSL VPN.....	239
L2TP.....	241
Routing.....	242
Static Routing.....	243
Policy Routing.....	246
Gateways.....	248
BGP.....	250
OSPF.....	251
Information.....	256
Upstream Proxy.....	269
Multicast (PIM-SIM).....	271
RIP.....	273
System Services.....	276
High Availability.....	277
Traffic Shaping Settings.....	284
RED.....	286
Log Settings.....	288
Data Anonymization.....	294
Traffic Shaping.....	297
Services.....	301
<b>Protect.....</b>	<b>303</b>
Firewall.....	303
User / Network Rule.....	306
Business Application Rule.....	318
Intrusion Prevention.....	374
DoS Attacks.....	374
IPS Policies.....	374
Custom IPS Signatures.....	378
DoS & Spoof Prevention.....	380
Web.....	390
Policies.....	390
User Activities.....	393
Categories.....	394
URL Groups.....	395
Exceptions.....	396
File Types.....	397
Surfing Quotas.....	398
User Notifications.....	401
Applications.....	401
Application List.....	401
Application Filter.....	402
Traffic Shaping Default.....	405
Wireless.....	405
Wireless Client List.....	405
Wireless Networks.....	406
Access Point Overview.....	409
Access Point Groups.....	415
Mesh Networks.....	417
Hotspots.....	419
Hotspot Voucher Definition.....	428
Rogue AP Scan.....	429
Wireless Settings.....	431
Hotspot Settings.....	432
Email.....	433

MTA Mode.....	434
Legacy Mode.....	461
Web Server.....	488
Web Servers.....	489
Protection Policies.....	490
Authentication Policies.....	494
Authentication Templates.....	497
SlowHTTP Protection.....	498
Advanced Threat.....	499
Advanced Threat Protection.....	499
Sandstorm Activity.....	500
Sandstorm Settings.....	501
Synchronized Security.....	501

## Appendix A - Logs.....503

Log Viewer.....	503
View List of System Events.....	505
View List of Web Filter Events.....	505
View List of Application Filter Events.....	506
View List of Malware Events.....	507
View List of Email Events.....	507
View List of Firewall Events.....	508
View List of IPS Events.....	509
View List of Authentication Events.....	510
View List of Admin Events.....	511
View List of Web Server Protection (WAF) Events.....	512
View List of Advanced Threat Protection Events.....	512
View List of Security Heartbeat Events.....	513
Log ID Structure.....	514
Log Type.....	514
Log Component.....	515
Log Subtype and Module Icons.....	517
Common Fields for all Logs.....	519
System Logs.....	520
Web Filter Logs.....	528
Module-specific Fields.....	528
Application Filter Logs.....	531
Module-specific Fields.....	531
Malware Logs.....	532
Module-specific Fields.....	532
Email Logs.....	533
Module-specific Fields.....	534
Firewall Logs.....	535
Module-specific Fields.....	537
IPS Logs.....	539
Module-specific Fields.....	539
Authentication Logs.....	541
Module-specific Fields.....	541
Admin Logs.....	542
Module-specific Fields.....	542
Sandstorm Logs.....	543
Web Server Protection (WAF) Logs.....	543
Advanced Threat Protection (ATP) Logs.....	543
Security Heartbeat Logs.....	543

<b>Appendix B - IPS - Custom Pattern Syntax.....</b>	<b>544</b>
<b>Appendix C - Default File Type Categories.....</b>	<b>550</b>
<b>Appendix E - Compatibility with SFMOS 15.01.0.....</b>	<b>554</b>
<b>Appendix F - Additional Documents.....</b>	<b>554</b>
<b>Copyright Notice.....</b>	<b>554</b>

# Introduction

---

Sophos XG Firewall provides unprecedented visibility into your network, users, and applications directly from the all-new control center. You also get rich on-box reporting and the option to add Sophos iView for centralized reporting across multiple firewalls.

Click [here](#) to view list of all features supported by Sophos XG Firewall.

## Flavors

---

This section provides information about different flavors available for Sophos XG Firewall.

Sophos is available in following flavors:

- Physical Devices
- Virtual Devices
- Software

### **Physical Devices**

Sophos provides a range of physical devices to cater the needs of all size of businesses i.e. small business to home users to enterprises.

### **Virtual Devices**

Virtual Network Security devices can be deployed as Next-Generation Firewalls or UTMs and offer industry-leading network security to virtual data-centers, “Security-in-a-Box” set-up for MSSPs/organizations, and “Office-in-a-Box” set-up. By offering comprehensive security features available in its hardware security devices, in virtualized form, these virtual devices offer Layer 8 Identity-based security on a single virtual device, which is as strong as security for the physical networks.

Sophos offers a complete virtual security solution to organizations with its virtual network security devices (Next-Generation Firewalls/UTMs), virtual Sophos Firewall Manager (SFM) for centralized management, and Sophos iView software for centralized logging and reporting.

## Administrative Interfaces

---

Device can be accessed and administered through:

- *[Admin Console](#)*: Admin Console is a web-based application that an Administrator can use to configure, monitor, and manage the Device.
- *[Command Line Interface](#)*: Command Line Interface (CLI) console provides a collection of tools to administer, monitor, and control certain component(s) of the device.
- *[Sophos Firewall Manager \(SFM\)](#)*: Distributed Sophos devices can be centrally managed using a single Sophos Firewall Manager (SFM) Device.

## Administrative Access

---

This section provides information on how to access Device.

An administrator can connect and access the device through HTTPS, telnet, or SSH services. Depending on the Administrator login account profile used for access, an administrator can access number of Administrative Interfaces and Admin Console configuration pages.

The device is shipped with one administrator account and four administrator profiles.

Administrator Type	Login Credentials	Console Access	Privileges
Super Administrator	admin/admin	Admin console CLI console	Full privileges for both the consoles. It provides read-write permission for all the configuration performed through either of the consoles.



**Note:** We recommend that you change the password of the user immediately on deployment.

## Admin Console

Admin Console is a web-based application that an Administrator can use to configure, monitor, and manage the Device.

You can connect to and access Admin Console of the device using HTTPS connection from any management computer using web browser:

1. HTTPS login: `https://<LAN IP Address of the device>`

For more details, refer to section [Admin Console](#).

## Command Line Interface (CLI) Console

CLI console provides a collection of tools to administer, monitor, and control certain component(s) of the device. The device can be accessed remotely using the following connections:

1. Remote login Utility – TELNET login
2. SSH Client (Serial Console)

Use CLI console for troubleshooting and diagnosing network problems in details.

## Sophos Firewall Manager (SFM)

Distributed Sophos devices can be centrally managed using a single Sophos Firewall Manager (SFM) Device, enabling high levels of security for MSSPs and large enterprises. To monitor and manage devices through SFM device you must:

1. Configure SFM in Sophos device.
2. Integrate Sophos device with SFM.

Once you have added the Devices and organized them into groups, you can configure single device or groups of devices.

# Using Admin Console

---

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

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

Services	Interface/Zones	Default Port
HTTPS	WAN	TCP Port 4444

The administrator can update the default ports for HTTPS service from **System > Administration > Admin Settings**

## **Admin Console Language**

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

Listed elements of Admin Console are displayed in the configured language:

- Control Center contents
- Navigation menu
- Screen elements including field & button labels and tips
- Error messages

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

All the configurations done from the Admin Console take effect immediately. To assist you in configuring the device, the device includes detailed context-sensitive online help.

## **Log on procedure**

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

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

Below are the screen elements with their description:

### **Username**

Enter user login name.

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

### **Password**

Specify user account password.

Dots are the placeholders in the password field.

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

### **Language**

Select the language. The available options are:

- Chinese-Simplified
- Chinese-Traditional
- English
- French
- Hindi
- German
- Italian
- Korean
- Brazilian Portuguese

Default – English

### **Log on to**

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

To login into your account, select **User Portal**.

### **Login button**

Click to log on the Admin Console.

Control Center appears as soon as you log on to the Admin Console. Control Center provides a quick and fast overview of all the important parameters of your device.

### Log out procedure

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

To log out of the device, navigate to **admin** at the top right of any of the Admin Console pages and click **Logout**.

## Supported Browsers

---

You can connect to Admin Console of the device using 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 10 onwards with JavaScript enabled.

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

## Menus

---

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 tabs. To view page associated with the tab, click the required tab.

The navigation menu includes following modules:

- Monitor & Analyze
- Protect
- Configure

- System

**Note:**

- Use F1 key for page specific help.

Each section in this guide shows the menu path to the configuration page. For example, to reach the High Availability page, choose System Services menu from Configure section in the navigation bar, and then choose High Availability tab. Online help mentions this path as:

**Configure > System Services > High Availability**

## Pages

---

A Leaf page is a page from where all the configurations can be done. The **admin** tab on the upper rightmost corner of every page provides access to several commonly used functions like:

1. **Support:** Opens the customer login page for creating a Technical Support Ticket. It is fast, easy and puts your case right into the Technical Support queue.
2. **About Product:** Opens the device registration information page.
3. **Wizard:** Opens the Network Configuration Wizard.
4. **Console:** Opens the Command Line Interface (CLI) console.
5. **Reboot Device:** Reboots the device.
6. **Shutdown Device:** Shut downs the device.
7. **Lock:** Locks the Admin Console. Admin Console is automatically locked if the device is in inactive state for more than 3 minutes. To unlock the Admin Console you need to relogin. By default, Lock functionality is disabled.  
Enable Admin Session Lock from **System > Administration > Settings**
8. **Logout:** Logs out from the Admin Console.

Clicking **Help** hyperlink on the upper rightmost corner of every page opens the content-sensitive help page.

Click **How-To Guides** to browse through our extensive library of how-to videos for XG Firewall.

## List Navigation Controls

---

The Admin Console pages display information in the form of lists and many lists are spread across the multiple pages. Page Navigation Controls at the bottom of the list provides navigation buttons for moving through list pages with large number of entries. It displays the current page and total number of pages.



## Monitor and Analyze

---

### Control Center

---

The Control Center appears as soon as you logon to the Admin Console.

Control Center provides a single screen snapshot of the state and health of the security system, which is easy to explore and drill.

## System Panel

System panel displays the real-time state of device services, VPN connections, WAN links and performance as well as number of days since the device is up and running. Status is displayed as an icon and colored icons are used to differentiate statuses. On clicking the icon, detailed information of the services is displayed.

The icons and their various status are:

### Performance Widget

Icon Status	
	Normal Load Average of the Device is less than 2 units.
	Warning Load Average is between 2 to 5 units.
	Alert Load Average more than 5 units.
	Unknown

On clicking the icon, the Load Average Graph of the device is displayed.

Load Average is a measure of the average number of processes waiting for execution time on a CPU. Any number greater than the number of processor cores in the system indicates that, during the time period being measured (for example, 5 minutes), there was generally more work to do than the system was capable of doing.

### Services Widget

Icon Status	
	Normal All the services are running.
	Warning One or more services has been explicitly stopped by the administrator. You can restart services from <b>Monitor &amp; Analyze &gt; System Services &gt; Services</b> .
	Alert One or more services is not running. You can restart services from <b>Monitor &amp; Analyze &gt; Services</b> .
	Unknown

On clicking the icon, the services that are stopped or dead are displayed.

### Interfaces Widget

Icon Status	
	Normal All the WAN links are UP.

Icon Status
 Warning 50% or less WAN links are DOWN.
 Alert 50% or more WAN links are DOWN.
 Unknown

On clicking the icon, details of WAN Links are displayed.

#### VPN Connections Widget

Icon Status
 Normal All the VPN tunnels are UP.
 Warning 50% or less VPN tunnels are DOWN.
 Alert 50% or more VPN tunnels are DOWN.
 Unknown

On clicking the icon, details of VPN tunnels are displayed.

#### CPU Widget

CPU graphs allow administrator to monitor the CPU usage by the Users and System components. Maximum and Average CPU usage is also displayed when clicked on the widget.

X-axis – Hours/Weeks/Months/Year (depending on the option selected)

Y-axis – % use

Click the widget to view details. Clicking any of the hyperlinks under **System Tools** and **Network Utilities** will redirect you to the respective page.

#### Memory Widget

Memory graphs allow administrator to monitor the memory usage in percentage. Graphs displays the memory used, free memory and total memory available. In addition, shows maximum and average memory usage.

X-axis – selected)

Y-axis – % use

Click the widget to view details. Clicking any of the hyperlinks under **System Tools** and **Network Utilities** will redirect you to the respective page.

#### Bandwidth Widget

Graph displays total data transfer through WAN Zone. In addition, shows maximum and average data transfer.

X axis – Hours/Days/Months/Year (depending on the option selected)

Y-axis – Total data transfer in KBits/Second

Click the widget to view details. Clicking any of the hyperlinks under **System Tools** and **Network Utilities** will redirect you to the respective page.

## Sessions Widget

Graph displays current sessions of the device. It also displays the maximum and average live connections.

Click the widget to view details. Clicking any of the hyperlinks under **System Tools** and **Network Utilities** will redirect you to the respective page.

## High Availability (HA) Details

Displays HA mode configured as below:

A-A : When device is configured in Active-Active mode.

A-P (M) : When device is configured in Active-Passive mode and is acting as Primary Device..

A-P (S) : When device is configured in Active-Passive mode and is acting as Auxiliary Device.

## Traffic Insight Panel

The section provides statistics related to network traffic processed by your device in the last 24 hours. The at a glance information helps find out who is consuming the most bandwidth, unusual traffic patterns, and most-visited websites and applications.

The statistics is displayed as bar graphs:

- Web Activity - The graph provides the user data transfer information over the last 24 hours, which helps in understanding the web surfing trend. It also displays the maximum and average amount of data transferred, in bytes, over the last 24 hours, which helps you spot unusual traffic patterns, if any. For example, if the graph displays a peak level at a certain point of time, it means the maximum amount of data transfer was done over that time period.
- Allowed App Categories - The graph displays the amount of data transferred, in bytes, for top five application categories. This information provides an administrator at a glance view of the most-used applications in the last 24 hours, which in turn helps you identify which applications consume the most bandwidth. Clicking on the bar of a particular application category in the graph will redirect you to the filtered application report of that category.
- Network Attacks - The graph lists top five hosts that were denied access to the network due to health reasons. Clicking on the bar of a particular attack category in the graph will redirect you to the filtered report of that category.
- Allowed Web Categories - The graph displays the amount of data transferred, in bytes, for top five web categories. This information provides an administrator at a glance view of the most-visited websites in the last 24 hours, which in turn helps you identify which websites consume the most bandwidth. Clicking on the bar of a particular web category in the graph will redirect you to the filtered report of that category.
- Blocked App Categories - The graph displays top five denied application categories along with number of hits per category. This way an administrator gets to know about the applications with the most number of failed access attempts. Clicking on the bar of a particular application category in the graph will redirect you to the filtered application report of that category.

## User & Device Insights Panel

### Security Heartbeat Widget

Security Heartbeat widget provides the health status of all endpoint devices. An endpoint device is an Internet-capable computer hardware device connected to Sophos XG Firewall via Sophos Central. The endpoint sends a heartbeat signal at regular intervals and also informs about potential threats to the Sophos XG Firewall.

If Security Heartbeat is not configured, the Configure button appears on the Control Center.

The health status of endpoint can be red, yellow, or green:

- Red labeled “At risk” - Active malware detected.
- Yellow labeled “Warning” - Inactive malware detected.
- Green (no label) - No malware detected.

- Red labeled “Missing” - Endpoints not sending health status information but causing network traffic.

Once Security Heartbeat is configured, all the endpoints are classified in either of the 4 status. The Security Heartbeat Widget shows the total number of endpoints in each status.

Click the widget to view the list of all endpoints with information like hostname/IP of the source, user and state changed. You can select to display all or just certain endpoints based on their health status.

#### Sandstorm Widget

Sophos Sandstorm is a cloud-based service that provides enhanced protection against malware. You can configure the firewall to send suspicious downloads to Sandstorm for analysis. Sandstorm detonates files to check for ransomware and other advanced threats. Because the analysis takes place in the cloud, your system is never exposed to potential threats.

Sandstorm requires a subscription. Click the link to start your free 30-day evaluation.

When Sandstorm is enabled, users will be prevented from downloading files that match the firewall criteria until the analysis is complete.

The Sandstorm widget displays analysis results for web traffic and email. Click the widget to view Sandstorm activity details.

#### Advanced Threat Protection Widget

Advanced Threat Protection widget provides a snapshot of advanced threats detected in your network. ATP can help rapidly detect infected or compromised clients inside the network and raise an alert or drop the respective traffic.

If Security Heartbeat is not configured, the Configure button appears on the Control Center.

Once configured, the widget will have either of the two status:

-  - Normal - No threats detected.
-  - Alert - It displays number of sources blocked. Clicking on it gives details like hostname/IP of the source, threat and count.

#### User Threat Quotient Widget

Widget displays the User Threat Quotient (UTQ) status of an organization aggregated for the last 7 days. This helps an administrator to get quick visibility of risky users, if any, who are posing security threats to the organization’s network.

Possible UTQ statuses:

-  - There are no users with risky web surfing behaviour or using infected hosts that are part of botnet.
-  - There are 13 users who are accounting for 80% of overall risk posed to the organization’s network.  
Note that the number 13 here is just an example and may vary from case to case. For example, there may be a case where single user is accounting for 80% of overall risk posed to the organization’s network! Click on this icon to view the User Threat Quotient (UTQ) reports for last 7 days.

#### RED Widget

Widget displays number of RED tunnels established and total number of RED tunnels configured in the form of 4/8. Click the widget to view list of RED tunnels.

#### Wireless APs Widget

Widget displays Active APs and total number of APs configured in the form of 2/3. Pending APs, if any will be displayed separately in a bracket in red color. Clicking the widget will redirect you to the **Access Points** page.

#### Connected Remote Users Widget

Widget displays total number of users connected remotely through SSL VPN. Clicking the widget, will redirect you to the **SSL VPN Users** page.

#### Live Users Widget

Widget displays total live users count. Clicking the widget, will redirect you to the **Live Users** page.

### Active Firewall Rules Panel

Active Firewall Rules panel displays information which can be used by the administrator to visualize and quantify (in terms of data volume) the firewall rules configured on the device. Using this information, the administrator can fine-tune the deployed firewall rules to troubleshoot or enhance network performance. All active firewall rules will be visible irrespective of the rights pertaining to the logged-on administrator profile.

#### Firewall Rule Types

Active Firewall Rules widget displays the number of firewall rules which are being used to process the network traffic, based on the following rule types:

- Business - Displays the number of active Business Application Firewall Rules
- User - Displays the number of active User Application Firewall Rules
- Network - Displays the number of active Network Firewall Rules

Total - Displays the total number of active firewall rules.

The chart displays the volume of data (in Bytes) processed by each active firewall rule type, in the last 24 hours. Hover over the chart area to see the volume of data processed by the active firewall rule type. Firewall Rule type is easily recognisable, based on the following legends:

- █ Business - Represented by Green area on the chart
- █ User - Represented by Red area on the chart
- █ Network - Represented by Blue area on the chart

Use the information in the chart area to determine the network saturation status and identify specific firewall rule type causing this.

#### Firewall Rule Status

The number of firewall rules, as per their current statuses are also displayed within the same widget. This is mainly for admin housekeeping purposes, also useful, where multiple administrators are working on the same device. The current statuses are based on the following categories or filters:

- Unused - Displays the number of firewall rules which does not process any traffic on the device. The administrator may want to revise unused firewall rules or delete them completely.
- Disabled - Displays the number of firewall rules which are configured on the device, but disabled by the administrator.
- Changed - Displays the number of firewall rules which have been updated recently.
- New - Displays the number of newly created firewall rules.

Clicking any of the Firewall Rule Types or Firewall Rule Status redirects to the Firewall page displaying the relevant firewall rules.

### Reports Panel

**Not applicable to - CR10iNG, CR10wiNG, CR15i, CR15wi, CR15iNG, CR15wiNG, CR15iNG-LE, CR15iNG-4P, CR15wiNG-4P, XG85 and XG85w models.**

Depending on the Modules subscribed, at most five critical reports from the below mentioned table are displayed:

Report Name	Number / Data Displayed	Subscription Module
High Risk Applications	<number of> Risky Apps seen yesterday	Web Protection
Objectionable Websites	<number of> Objectionable websites seen yesterday	Web Protection
Web Users	<data transfer> (in bytes) used by top 10 users yesterday	Web Protection
Intrusion Attacks	<number of> Intrusion attacks yesterday	Network Protection
Web Server Protection	<number of> Web server attacks yesterday	Web Server Protection
Email Usage	<data transfer> (in bytes) used	Email Protection
Email Protection	<number of> Spam mails yesterday	Email Protection
Traffic Dashboard	-	Either Web Protection or Network Protection
Security Dashboard	-	Either Web Protection or Network Protection

### Prevalent Malware Panel

Applicable to CR15iNG, CR15wiNG, CR15i and CR15wi models only

Displays top five malware identified by the Device, in addition to the number of occurrence per malware.

### Messages Panel

Panel displays information which allows administrator to monitor and track the system events of the device. Each message displays the date and time that the event occurred.

Displays following alerts:

1. The default password for the user “admin” has not been changed. We highly recommend you to change the password. – This alert is displayed when default password for super administrator is not changed.
2. The default Admin Console password has not been changed.
3. HTTPS, SSH based management is allowed from the WAN. This is not a secure configuration. We recommend using a good password.
4. HTTP, Telnet based management is allowed from the WAN. This is not a secure configuration. We recommend using a good password.
5. Your Device is not registered.
6. The modules expired.

Symbolic representations are used for easier identification of messages.

 : Indicates Alert messages.

 : Indicates warnings.

 : Indicates firmware download notifications.

## Connections and Interfaces

The image of the device will be displayed in this panel on the right side. For a virtual device, stack of devices will be displayed.

### Interface Table

This panel displays information of Interfaces describing their Name, Type and Status, Received and Transmitted KBits/s.

Displays following details:

1. Interface - This displays the name of the Interface configured in the system. Example Port A, Guest AP. It displays Physical, LAG and Bridge type of Interfaces.
2. Type - This displays the zone along with the type of Interface configured. Example LAN-Physical, WAN-VLAN etc.
3. Status - This displays the status and the Interface Speed for the configured Interface. Status can be connected, unplugged, disconnected, connecting, enabled or disabled (for RED interface only).
4. Received Kbits/s - This displays the received bits through the Interface.
5. Transmitted Kbits/s - This displays the transmitted bits through the Interface.

### Gateway Table

This panel displays information of Gateways which allows administrator to monitor Active and Backup Gateways describing their Name, Interface, Type, IPv4/IPv6, Activate on Failure of, Weight and Status.

Displays following details:

1. Gateway Name - This displays the name of the Gateway.
2. Interface - This displays the name and IP address of the Interface.
3. Type - This displays the type of the Gateway in terms of load balancing. Available options are Active and Backup.
4. IPv4/IPv6 - This displays the type of the Gateway in terms of IP addressing type used. Available options are IPv4 and IPv6.
5. Activate on Failure of - This displays the action for the Gateway failure situation, i.e. whether a backup Gateway will be activated or not.
6. Weight - This displays that how much traffic will pass through a particular link in relation to the other link(s).
7. Status - This displays the status of the Gateway. Status can be Active, Deactive.

---

## Current Activities

The **Current Activity** section provides information about the live IPsec, SSL, IP and wireless connections to the device.

- *[Live Users](#)*: Displays a list of all the users currently connected to the device.
- *[IPsec Connections](#)*: Displays a list of all the live IPsec connections.
- *[Remote Users](#)*: Displays a list of all the live SSL VPN users.
- *[Live Connections IPv4](#)*: Displays a list of the live IPv4 connections on the device. You can forcefully disconnect the connections from the respective pages.
- *[Live Connections IPv6](#)*: Displays a list of the live IPv6 connections on the device. You can forcefully disconnect the connections from the respective pages.

## Live Users

Live users in the device can be managed from a single page. All the active normal users, clientless users and single sign-on users are visible from the **Live Users** page. The administrator can disconnect these users from this page directly.

User Types:

- Normal
- Clientless
- Single Sign-On
- Thin Client
- WWAN user

A normal user has to logon to the device. It requires a client (client.exe) on the user machine or a HTTP client component can be used and all the policy-based restriction are applied.

A clientless user does not require a client component (client.exe) on the user machines.

If a user is configured for single sign-on, whenever the user logs on to Windows, he/she is automatically logged to the device.

If the user is a thin client user, whenever the user logs on, this is visible on the **Live Users** page.

If a wireless user is configured and connected, the user is shown on the **Live Users** page.

To disconnect a user:

1. Click the Disconnect icon  under the Manage column against a user.
2. Specify the message in a dialog box.
3. Click **OK** to disconnect the user. To disconnect multiple live users, select them and click **Disconnect**.

 **Note:** Configured messages will not be sent to a clientless user.

<input type="checkbox"/>	User ID	Username	Client Type	Host IP	IP Family	MAC	Start Time	Upload	Download
<input type="checkbox"/>	9	<a href="#">printer</a>	Clientless	10.10.10.5	IPv4	-	2015-10-25 23:45	0.00 KB	0.00 KB

**Figure 1: Live Users**

### Related Topics

[Users](#) on page 182

The Users page displays the list of all users added in the device.

## Live Connections

Use **Live Connections** page to view a list of all currently active IPv4 connections.

The page displays the IPv4 live connections report and offers to get a quick real-time statistics of the network traffic.

You can use this report to check the share in network load of different protocols, computer systems (in your LAN or in the Internet), connections, or a combination of these (e.g. network connections with a certain protocol). Drill down quickly to get an in-depth view of your network.

### Connections per Application

Use to determine the amount of traffic generated (bandwidth used) by application in real-time. It also displays which user is using which application currently and total data transferred using the application.

Use to view:

- [Connection Details per Application](#)
- [Connections Details per Application and Username](#)

For each connection the list shows:

### Application

Applications running on network.

Click number in **Total Connections** column against application to view destination IP address-wise and destination port-wise connection details for the selected application.

Click the icon to view list of users using the respective application or click the icon to hide the list of users.

#### **Upload Transfer**

Data uploaded through the application.

#### **Download Transfer**

Data downloaded through the application.

#### **Upstream Bandwidth**

Upstream bandwidth.

#### **Downstream Bandwidth**

Downstream bandwidth.

#### **Total Connections**

Displays number of connections initiating/requesting the application.

Click the number in the **Total Connections** column to view the connection details for the selected application.

Application	Upload Transfer	Download Transfer	Upstream Bandwidth	Downstream Bandwidth	Total Connections
GOOGLE PLUS WEBSITE	2.70 KB	6.63 KB	22 Bytes/Sec	56 Bytes/Sec	1

**Figure 2: Live Connections based on Application**

#### **Connections per User**

Used to determine the amount of traffic generated (bandwidth used) by users in real time i.e. traffic per user. It also displays which user is using a particular application currently and is consuming how much bandwidth.

Use to view:

- *Connection Details per User*
- *Connections Details per User and Application*

For each connection the list shows:

#### **User**

Network Users requesting various Applications.

Click to view list of applications or click icon to hide the list of applications.

Click number in **Total Connections** column against user to view

Click User to view Destination IP Addresses wise and Destination ports wise Connection details for selected User.

#### **Upload Transfer**

Data uploaded.

#### **Download Transfer**

Data downloaded.

#### **Upstream Bandwidth**

Upstream bandwidth.

#### **Downstream Bandwidth**

Downstream bandwidth.

## Total Connections

Displays number of connections initiated by the User.

Click **Total Connections** to view the connection details for selected User.

User	Upload Transfer	Download Transfer	Upstream Bandwidth	Downstream Bandwidth	Total Connections
+ NA	328.57 KB	898.78 KB	6 Bytes/Sec	17 Bytes/Sec	<u>25</u>

**Figure 3: Live Connections IPv4 based on Username**

## Connections per Source IP Address

Use to determine the amount of traffic generated (bandwidth used) by source IP addresses in real time i.e. traffic per source IP address. It also displays which user is using a particular application currently and is consuming how much bandwidth.

Use to view:

- *Connection Details*
- *Connection per Source IP Address and Application*

### Source IP Address

Source IPv4 Addresses requesting various applications.

Click to view list of Source IPv4 Addresses or click to hide the list of IP Addresses.

### Upload Transfer

Data uploaded.

### Download Transfer

Data downloaded.

### Upstream Bandwidth

Upstream bandwidth.

### Downstream Bandwidth

Downstream bandwidth.

### Total Connections

Displays number of connections initiated by the Source IP Address.

Click **Total Connections** to view the connection details for selected User.

Source IP Address	Upload Transfer	Download Transfer	Upstream Bandwidth	Downstream Bandwidth	Total Connections
+ 10.10.10.8	28.43 KB	5.48 KB	9 Bytes/Sec	1 Bytes/Sec	1

**Figure 4: Live Connections IPv6 based on Source IP**

## Live Connections IPv6

Use **Live Connections IPv6** page to view a list of all currently active IPv6 connections.

The page displays the IPv6 live connections report and offers to get a quick real-time statistics of the network traffic.

You can use this report to check the share in network load of different protocols, computer systems (in your LAN or in the Internet), connections, or a combination of these (e.g. network connections with a certain protocol). Drill down quickly to get an in-depth view of your network.

## Connections per User

Used to determine the amount of traffic generated (bandwidth used) by users in real time i.e. traffic per user. It also displays which user is using a particular application currently and is consuming how much bandwidth.

Use to view:

- [Connection Details per User](#)
- [Connections Details per User and Application](#)

For each connection the list shows:

### User

Network users requesting various applications

Click the  icon to view the list of applications used by the user or click the  icon to hide the list of applications.

Click number in **Total Connections** column against user to view destination IP address-wise and destination port-wise connection details for the selected user.

### Upload Transfer

Data uploaded.

### Download Transfer

Data downloaded.

### Upstream Bandwidth

Upstream bandwidth.

### Downstream Bandwidth

Downstream bandwidth.

### Total Connections

Displays the number of connections initiated by the user.

Click the number in the **Total Connections** column to view the connection details for the selected user.

User	Upload Transfer	Download Transfer	Upstream Bandwidth	Downstream Bandwidth	Total Connections
 NA	328.57 KB	898.78 KB	6 Bytes/Sec	17 Bytes/Sec	<a href="#">25</a>

**Figure 5: Live Connections IPv6 based on User**

## Connections per Source IP Address

Use to determine the amount of traffic generated (bandwidth used) by source IP addresses in real time i.e. traffic per source IP address. It also displays which user is using a particular application currently and is consuming how much bandwidth.

Use to view:

- [Connection Details](#)
- [Connection per Source IP Address and Application](#)

### Source IP Address

Source IPv6 Addresses requesting various applications.

Click  to view list of Source IPv6 Addresses or click  to hide the list of IP Addresses.

### Upload Transfer

Data uploaded.

### Download Transfer

Data downloaded.

### Upstream Bandwidth

Upstream bandwidth.

### Downstream Bandwidth

Downstream bandwidth.

### Total Connections

Displays number of connections initiated by the Source IP Address.

Click **Total Connections** to view the connection details for selected User.

Source IP Address	Upload Transfer	Download Transfer	Upstream Bandwidth	Downstream Bandwidth	Total Connections
+ 2001:cdba::3257:9652	29.07 KB	5.84 KB	6 Bytes/Sec	1 Bytes/Sec	1

**Figure 6: Live Connections IPv6 based on Source IP**

## View Live Connection Details

The page displays the connection details per application, user, and source IP address.

### Connection Details for the Selected Application

Click on the **Total Connections** link against the application to view its connection details.

#### Start Time

Time when connection was established.

#### In Interface

Traffic incoming interface.

#### Out Interface

Traffic outgoing interface.

#### Source IP

IP address from which the connection for the application was established.

#### Destination IP

IP address to which the connection was established.

#### Protocol

Protocol used by the traffic.

#### Source Port

Port through which the connection was established for the application.

#### Destination Port

Port to which the connection was established for the application.

#### Rule ID

Firewall rule ID applied to the connection traffic.

#### Upload Transfer

Data uploaded.

#### Download Transfer

Data downloaded.

#### **Upstream Bandwidth**

Upstream bandwidth.

#### **Downstream Bandwidth**

Downstream bandwidth.

### **Connection Details for the Selected Application and User**

Click on the **Total Connections** link against the user name to view the connection details of the connections established by the user for the selected application.

#### **Start Time**

Time when connection was established.

#### **In Interface**

Traffic incoming interface.

#### **Out Interface**

Traffic outgoing interface.

#### **Source IP**

IP address from which the connection for the application was established.

#### **Destination IP**

IP address to which the connection was established.

#### **Protocol**

Protocol used by the traffic.

#### **Source Port**

Port through which the connection was established for the application.

#### **Destination Port**

Port to which the connection was established for the application.

#### **Rule ID**

Firewall rule ID applied to the connection traffic.

#### **Upload Transfer**

Data uploaded.

#### **Download Transfer**

Data downloaded.

#### **Upstream Bandwidth**

Upstream bandwidth.

#### **Downstream Bandwidth**

Downstream bandwidth.

### **Connection Details for the Selected User and Application**

Click on the **Total Connections** link against the application to view the connection details of the connections established by the applications for the selected user.

#### **Start Time**

Time when the connection was established.

#### **In Interface**

Traffic incoming interface.

**Out Interface**

Traffic outgoing interface.

**Source IP**

IP address from which the connection for the application was established.

**Destination IP**

IP address to which the connection was established.

**Protocol**

Protocol used by the traffic.

**Source Port**

Port through which the connection was established for the application.

**Destination Port**

Port to which the connection was established for the application.

**Rule ID**

Firewall rule ID applied to the connection traffic.

**Upload Transfer**

Data uploaded.

**Download Transfer**

Data downloaded.

**Upstream Bandwidth**

Upstream bandwidth.

**Downstream Bandwidth**

Downstream bandwidth.

**Connection Details of the Selected User**

Click on the **Total Connections** link against the user to view its connection details.

**Start Time**

Time when the connection was established.

**In Interface**

Traffic incoming interface.

**Out Interface**

Traffic outgoing interface.

**Source IP**

IP address from which the connection for the user was established.

**Destination IP**

IP address to which the connection was established.

**Protocol**

Protocol used by the traffic.

**Source Port**

Port through which the connection was established for the user.

**Destination Port**

Port to which the connection was established for the user.

**Rule ID**

Firewall rule ID applied to the connection traffic.

**Upload Transfer**

Data uploaded.

**Download Transfer**

Data downloaded.

**Upstream Bandwidth**

Upstream bandwidth.

**Downstream Bandwidth**

Downstream bandwidth.

**Connection Details of the Selected Source IP Address**

Click on the **Total Connections** link against the source IP address to view its connection details.

**Start Time**

Time when the connection was established.

**In Interface**

Traffic incoming interface.

**Out Interface**

Traffic outgoing interface.

**Source IP**

IP address from which the connection for the source IP address was established.

**Destination IP**

IP address to which the connection was established.

**Protocol**

Protocol used by the traffic.

**Source Port**

Port through which the connection was established for the source IP address.

**Destination Port**

Port to which the connection was established for the source IP address.

**Rule ID**

Firewall rule ID applied to the connection traffic.

**Upload Transfer**

Data uploaded.

**Download Transfer**

Data downloaded.

**Upstream Bandwidth**

Upstream bandwidth.

**Downstream Bandwidth**

Downstream bandwidth.

**Connection Details of the Selected Application and Source IP Address**

Click on the **Total Connections** link against the application to view the connection details of the connections established by the application from the selected source IP address.

**Start Time**

Time when the connection was established.

**In Interface**

Traffic incoming interface.

#### **Out Interface**

Traffic outgoing interface.

#### **Source IP**

IP address from which the connection for the application was established.

#### **Destination IP**

IP address to which connection was established.

#### **Protocol**

Protocol used by the traffic.

#### **Source Port**

Port through which the connection was established for the application.

#### **Destination Port**

Port to which the connection was established for the application.

#### **Rule ID**

Firewall rule ID applied to the connection traffic.

#### **Upload Transfer**

Data uploaded.

#### **Download Transfer**

Data downloaded.

#### **Upstream Bandwidth**

Upstream bandwidth.

#### **Downstream Bandwidth**

Downstream bandwidth.

## **IPsec Connections**

The page displays list of all the connected IPsec tunnels and you can filter the list based on connection name, local server name, local subnet, user name, remote server/host or remote subnet.

To view the IPsec connection, go to **Monitor & Analyze > Current Activities > IPsec Connections**. The administrator can disconnect any of the IPsec connection if required by clicking **Disconnect** or update the list by clicking **Refresh**.

The table **IPsec Connections** contains the following information:

- **Name:** Name of the IPsec connection.
- **Local Sever:** Name of the local server.
- **Local Subnet:** Name of the local subnet.
- **Username:** Name of the IPsec connection user.
- **Remote Sever/Host:** Name of the Remote Server/Host.
- **Remote Subnet:** Name of the Subnet.

#### **Related Topics**

[IPsec Connections](#) on page 212

The **IPsec** menu allows you to create and manage IPsec connections and failover groups.

## **Remote Users**

Use **Remote Users** page to view a list of active remote users.

To view Remote Users page, go to **Monitor & Analyze > Current Activities > Remote Users**.

The page displays a list of all the currently logged remote users and you can filter the connections based on the connection date, username, source IP address, or leased IP address.

The administrator can disconnect any of the remote users, if required, by clicking **Disconnect**.

### Related Topics

[Add SSL VPN Remote Access Policy](#) on page 219

This page allows adding SSL VPN remote access policies.

## Diagnostics

---

This menu allows checking the health of your device in a single shot. Information can be used for troubleshooting and diagnosing problems found in your device.

Use this menu to configure below details:

- [Tools](#) - View the statistics to diagnose the connectivity problem, network problem and test network communication. It assists in troubleshooting issues such as hangs, packet loss, connectivity, discrepancies in the network. Also, troubleshooting reports can be generated to debug system problems.
- [System Graphs](#) - Use to view graphs pertaining to the system related activities for different time intervals.
- [URL Category Lookup](#) - Use to search whether the URL is categorized or not.
- [Packet Capture](#) - Displays packets details on the specified interface.
- [Connection List](#) - Provides current or live connection snapshot of your device in the list form.
- [Support Access](#) - Use this page to grant support staff temporary access to your device.

## Tools

Using the **Tools** page, one can view the statistics to diagnose the connectivity problem, network problem and test network communication. It assists in troubleshooting issues such as hangs, packet loss, connectivity, discrepancies in the network. The page covers:

- [Ping](#)
- [Traceroute](#)
- [Name Lookup](#)
- [Route Lookup](#)
- [Consolidated Troubleshooting Report](#)

### Ping

Ping is the 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 the 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 the address is reachable or not
- Check how long it takes to get a response
- Get the IP address from the domain name
- Check for the packet loss

The parameters used are:

#### IP Address/Host Name

Specify the IP address (IPv4/IPv6) or fully qualified domain name to be pinged.

Ping determines the network connection between the device and a 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.

#### IP Family

Select the type of IP family from the options available:

**Available Options** IPv4 IPv6

#### Interface

Select the interface through which the ICMP echo requests are to be sent.

#### Size

Specify the ping packet size, in bytes.

Default: 32 bytes

Size Range: 1 to 65507

The screenshot shows a configuration form for a ping operation. The fields are as follows:

- IP Address/Hostname \***: An input field for specifying the target address.
- IP Family \***: A radio button group where **IPv4** is selected and **IPv6** is unselected.
- Interface**: A dropdown menu labeled "Select Interface".
- Size**: An input field containing the value "[1-65507]".
- Ping**: A blue button at the bottom left of the form.

**Figure 7: Ping**

#### Traceroute

Traceroute is a useful tool to determine if a packet or communication stream is being stopped at the device, 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 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.

The parameters used are:

#### IP Address/Host Name

Specify the IP address (IPv4/IPv6) or fully qualified domain name.

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

#### IP Family

Select the type of IP family from the options available:

**Available Options** IPv4 IPv6

#### Interface

Select the interface through which the requests are to be sent.

IP Address/Hostname \*

IP Family \*  IPv4  IPv6

Interface

**Traceroute**

**Figure 8: Traceroute**

### 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 a domain name is entered, the return is an IP address to which it corresponds, and if an IP address is entered, then the domain name is returned to which it corresponds. In other words, Name Lookup reaches out over the Internet to do a DNS lookup from an authorized name server, and displays the information in user understandable format.

The parameters used and their descriptions are:

**IP Address/Host Name**

IP address (IPv4/IPv6) or fully qualified domain name that needs to be resolved.

**DNS Server IP**

Select the DNS server to which the query is to be sent.

Select **Lookup using all Configured Servers** to view all the available DNS servers configured in the device. Selecting this option will also provide information about the time taken by each DNS sever to resolve the query. Based on the response time,of each server, you can prioritize the DNS server.

IP Address/Hostname \*

DNS Server IP \*

**Name Lookup**

**Figure 9: Name Lookup**

### Route Lookup

If you have routable networks and wish to search through which interface the device routes the traffic then lookup the route for the IP address (IPv4/IPv6).

IP Address \*

**Route Lookup**

**Figure 10: Route Lookup**

## Consolidated Troubleshooting Report

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

The administrator has to generate and mail the saved file to Support for diagnosing and troubleshooting the issue.

The file will be generated with the name: CTR\_<APPKEY>\_<MM\_DD\_YY>\_<HH\_MM\_SS> where

- APPKEY is the device key of the device for which the report is generated
- MM\_DD\_YY is the date (month date year) on which the report is generated
- HH\_MM\_SS is the time (hour minute second) at which the report is generated

By default, the debug mode is off for all the subsystems. Before generating a log file, enable the debug mode by executing following command at the command line:

```
console> diagnostics subsystems <subsystem name> debug on
```

 **Note:** Debug mode cannot be enabled, if you only want to generate a system snapshot.

The parameters used are:

### Generate CTR for

Enable the option(s) for which CTR should be generated.

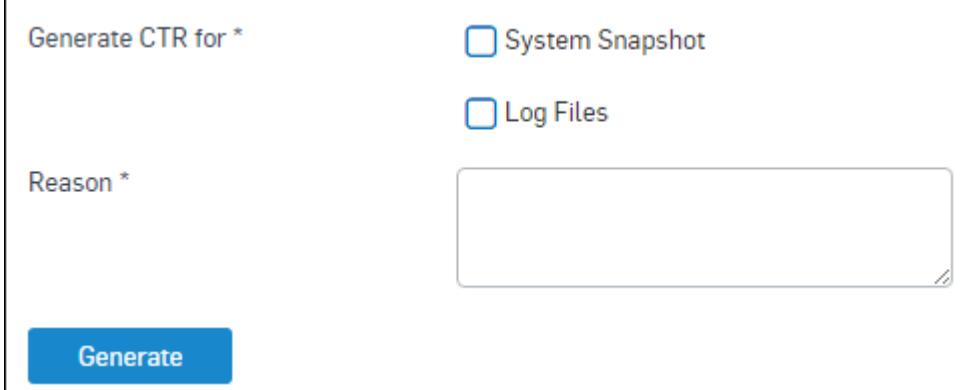
**Available Options:** **System Snapshot:** Generates snapshots to display the issues in the system. **Log Files:** Generates log files.

### Reason

Specify the reason for generating CTR.

### Generate

Click to generate the CTR.



Generate CTR for \*

System Snapshot

Log Files

Reason \*

Generate

**Figure 11: Consolidated Troubleshooting Report**

## System Graphs

**System Graphs** page displays graphs pertaining to system related activities for different time intervals.

### Monitor & Analyze > Diagnostics > System Graphs

System graphs displays following information for the selected period. These graphs are same as displayed in Utility wise graphs. They are regrouped based on the time interval.

1. [CPU usage info](#)
2. [Memory usage info](#)
3. [Load average](#)
4. [Disk usage](#)

5. [Number of live users](#)
6. [Data transfer through WAN zone](#)
7. [Interface usage Info](#)

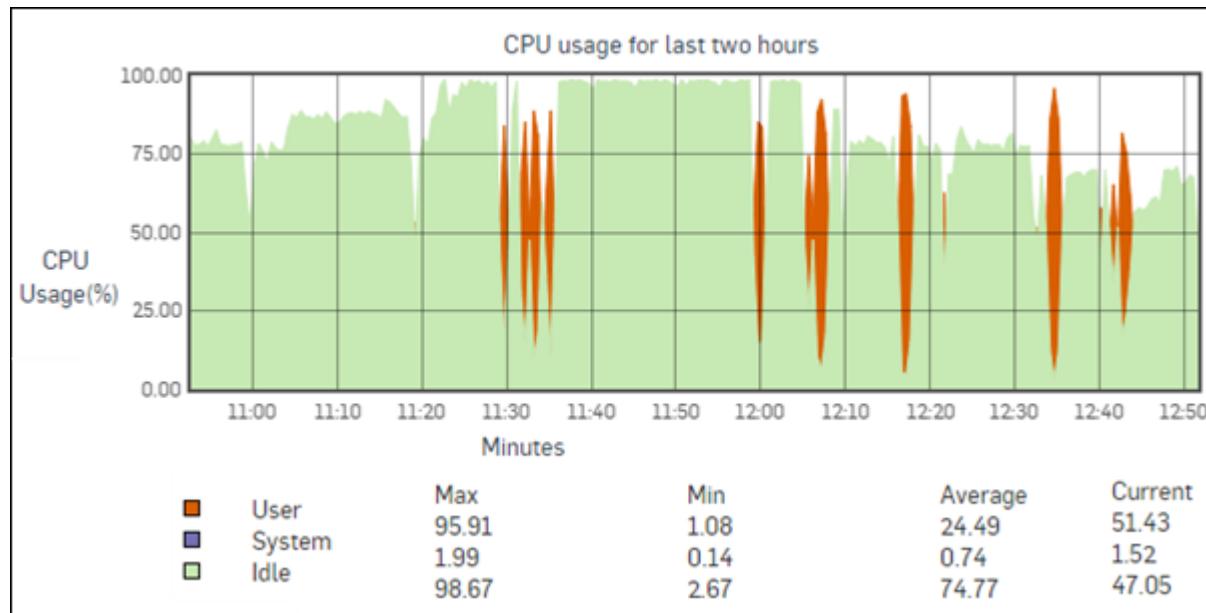
## CPU Usage Graphs

**CPU Usage** graphs enable the administrator to monitor the CPU usage by the users and system components. Graphs display percentage wise minimum, maximum, average and current CPU usage for user, system, and CPU idle time.

- X-axis –Minutes/hours/days/months (depending on the period selected)
- Y-axis – % use

Legend:

- Orange color – CPU used by user
- Purple color – CPU used by system
- Green color – CPU idle time



**Figure 12: CPU Usage**

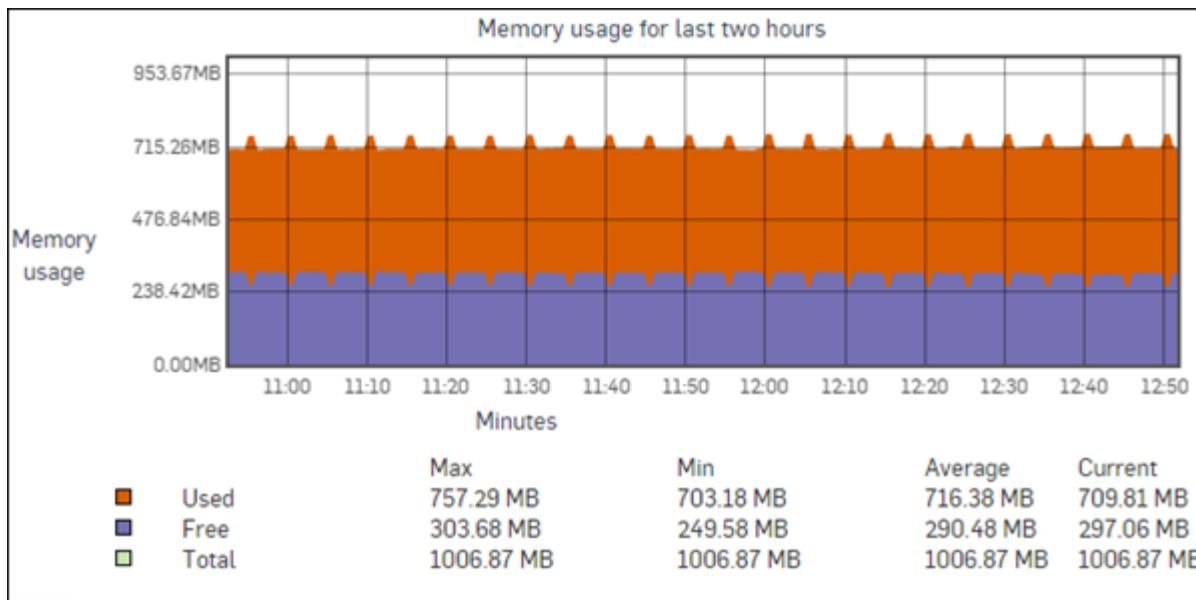
## Memory Usage Graphs

**Memory Usage** graphs enable the administrator to monitor the memory usage in Megabytes(MB). Graph displays percentage wise minimum, maximum, average and current memory used, free memory and total memory available.

- X-axis –Minutes/hours/days/months (depending on the period selected)
- Y-axis – Memory used in MB

Legend:

- Orange color – Memory used
- Purple color – Free memory
- Green color – Total memory



**Figure 13: Memory usage**

### Load Average Graphs

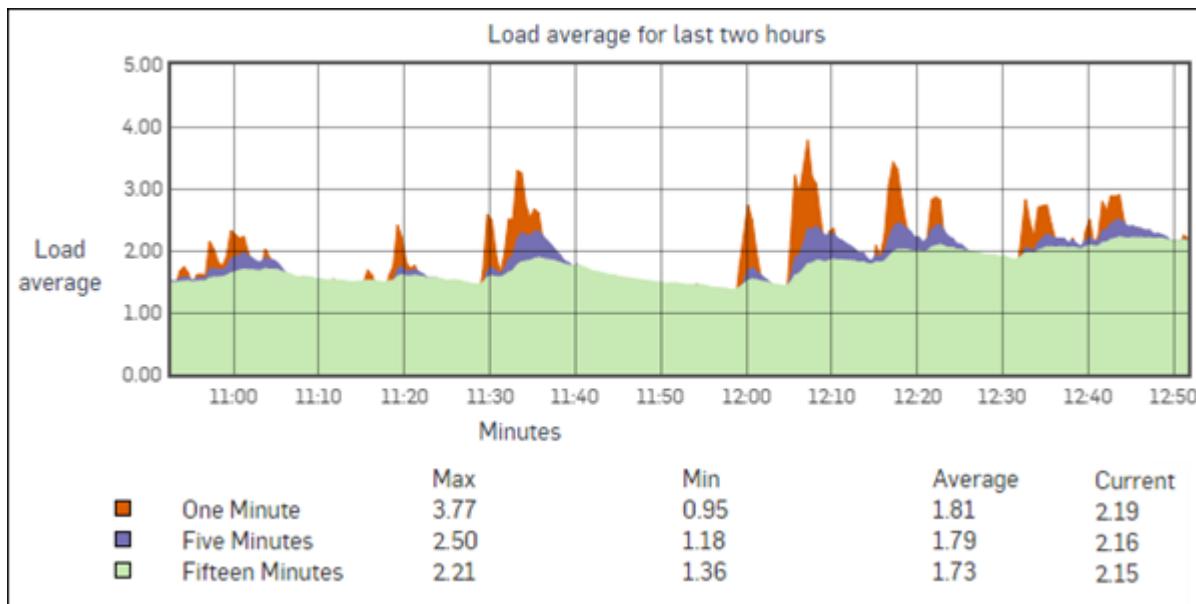
Load Average graphs enables the administrator to monitor the load on the system.

Graphs display the minimum, maximum, average and current load on the system at the interval of one minute, five minutes, and fifteen minutes.

- X-axis –Minutes/hours/days/months (depending on the period selected)
- Y-axis – Load average index

Legend:

- Orange color – One minute
- Purple color – Five minutes
- Green color – Fifteen minutes



**Figure 14: Load Average**

## Disk Usage Graphs

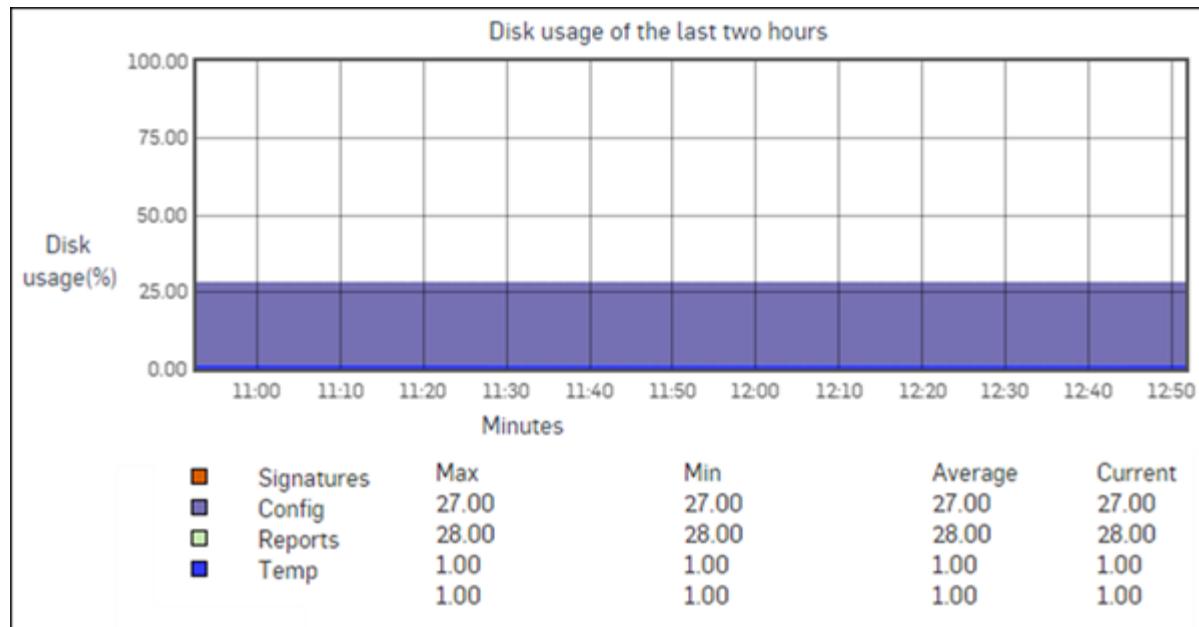
Disk Usage graphs enable the administrator to monitor the disk usage in percentage.

Graphs display the minimum, maximum, average and currently used disk space in percentage by Signatures, Config, Reports and Temp files.

- X-axis –Minutes/hours/days/months (depending on the period selected)
- Y-axis – % use

Legend

- Orange color – Disk space used by signatures
- Purple color – Disk space used by config files
- Green color – Disk space used by reports
- Blue color – Disk space used by temp



**Figure 15: Disk Usage**

## Live Users Graphs

Live Users graphs enable the administrator to monitor the number of live users for the selected time duration.

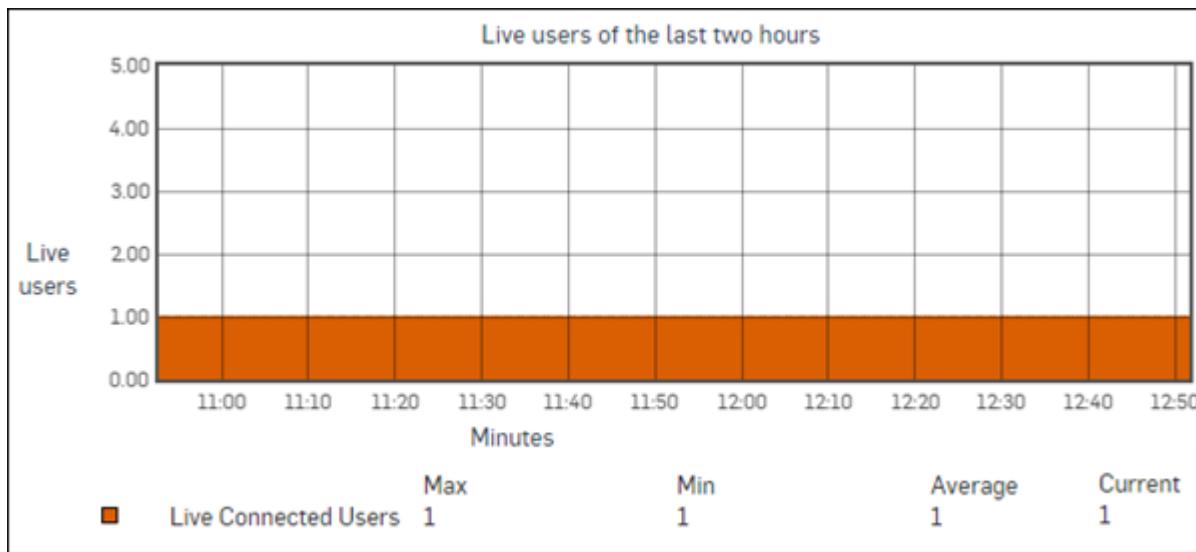
Graphs display the number of users currently connected to the Internet. In addition, it shows the minimum, maximum and average number of users connected during the selected period.

This helps the administrator in determining the peak hour of the day.

- X-axis –Minutes/hours/days/months (depending on the period selected)
- Y-axis – Numbers of users

Legend

- Orange color – Number of live connected users



**Figure 16: Live Users**

### Data Transfer through WAN Zone Graphs

**Data Transfer** for WAN zone graphs is subdivided into three (3) graphs providing various information about data transfer via WAN zone.

1. **Total upload/download data transfer of the selected period** – Graph displays combined graph of upload & download data transfer. Colors differentiate upload & download data traffic. In addition, it shows the minimum, maximum and average data transfer for upload & download traffic individually.
  - X-axis –Minutes/hours/days/months (depending on the period selected)
  - Y-axis – Upload/download in KBits/second

#### Legend

- Orange Color - Upload traffic

2. **Total data transfer of the selected period** - Graph displays the total data transfer from the WAN zone. In addition, it shows the minimum, maximum and average data transfer.
  - X-axis –Minutes/hours/days/months (depending on the period selected)
  - Y-axis – Upload/download in KBits/second

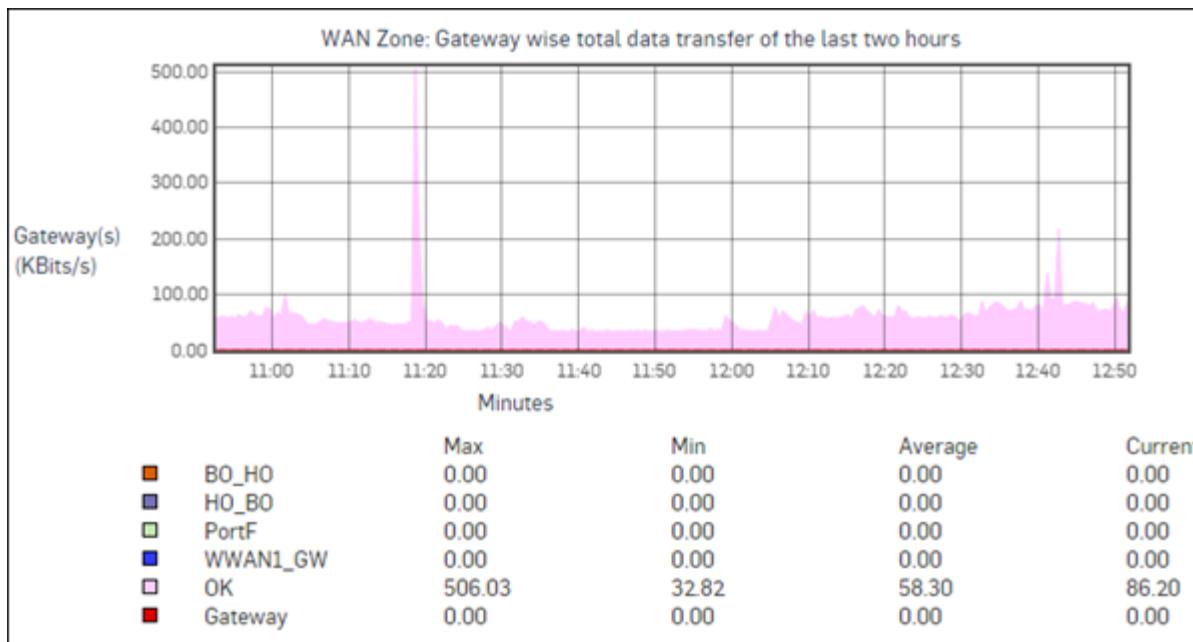
#### Legend

- Orange Color - Total (upload + download) traffic
- Purple Color - Download traffic

3. **Gateway wise total data transfer of the selected period** - Graph displays the gateway-wise data transfer from the WAN zone. In addition, it shows the minimum, maximum and average data transfer of each gateway.
  - X-axis –Minutes/hours/days/months (depending on the period selected)
  - Y-axis – Upload/download in KBits/second

#### Legend

- Different color for each gateway



**Figure 17: WAN Data Transfer**

### Interface Info Graphs

**Interface Info** graph displays following traffic statistics for all the interfaces - physical interfaces, VLAN interfaces, wireless LAN and WAN interfaces:

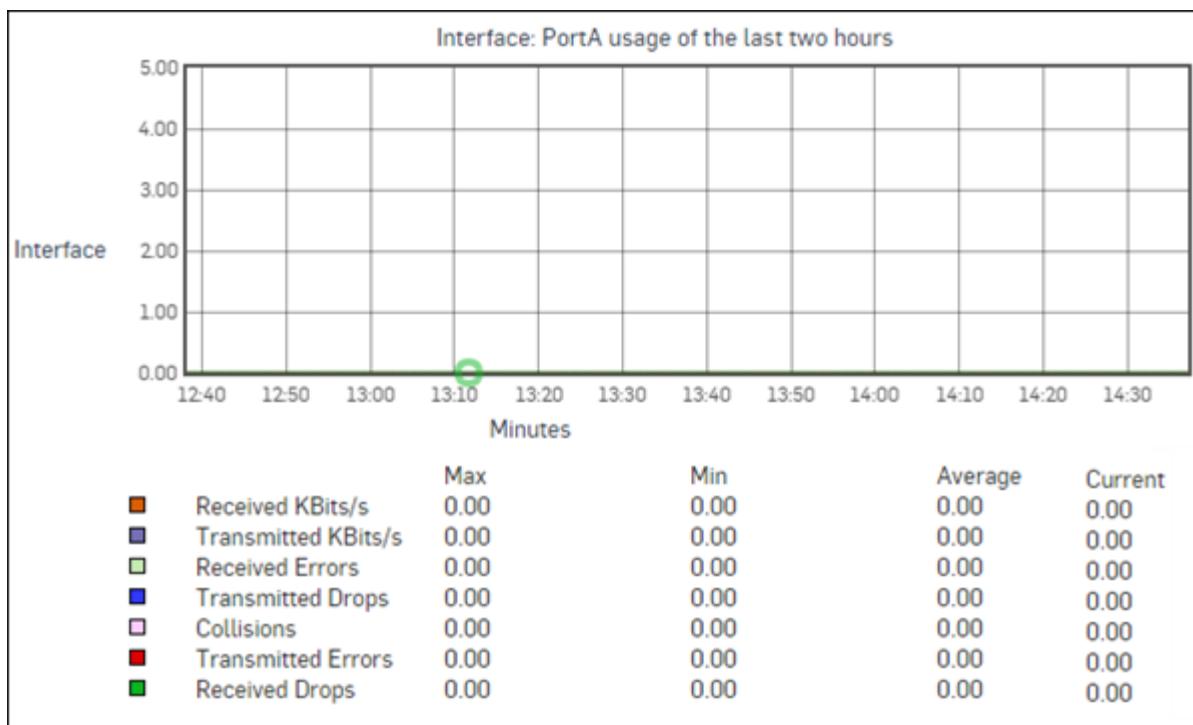
1. Bits received and transmitted through the interface
2. Errors occurred while transmitting and receiving packets through the interface
3. Packets dropped while transmitting and receiving packets through the interface
4. Collisions occurred while transmitting and receiving packets through the interface

The graph shows

- X-axis – Minutes/hours/days/months (depending on the period selected)
- Y-axis – KBits/sec

#### Legend

- Orange color – Bits received (kbits/sec)
- Purple color – Bits transmitted (kbits/sec)
- Light Green color – Received Errors (kbits/sec)
- Blue color – Bits transmitted but dropped
- Pink color – Collisions
- Red color – Transmitted errors
- Dark Green color – Bits received but dropped



**Figure 18: Interface Graph**



#### Note:

- Today and Yesterday graphs are plotted at the average of 5 minutes.
- Weekly graph is plotted at the average of 15 minutes.
- Monthly graph is plotted at the average of 6 hours
- Yearly graph is plotted at the average of 1 day

## URL Category Lookup

Use **URL Category Lookup** to search whether the URL is categorized or not. It searches the specified URL and displays the category name under which the URL is categorized along with the category description.

If domain/URL is categorized under both a Custom Category and a Default Category, then name of the Custom Category will be displayed in the search result.

To search a URL:

1. Go to **Monitor & Analyze > Diagnostics > URL Category Lookup**.
2. Enter URL to be searched in **Search URL**.
3. Click **Search**.

\*
Search URL \*

Search

**Figure 19: URL Category Lookup**

## Packet Capture

This page displays packets details on the specified interface. It will provide connection details and details of the packets processed by each module packets e.g. firewall, IPS along with information like firewall rule number, user, web and application filter policy number etc. This will help administrators to troubleshoot errant firewall rules.

You can:

- [Configure Capture Filter](#) – Configure filter settings for capturing the packets.
- [View](#) – View the packet information.
- [Display Filter](#) – Specify the filter conditions for the packets.
- Start/Stop – Start and stop packet capturing.
- Refresh – Refresh the list.
- Clear – Clear the details of the packets captured.

## Packet Capture

### Trace On/Off

Click the slider to enable/disable packet capturing.

The status, the buffer size and buffer used for capturing is displayed:

- Trace On - packet capturing is on.
- Trace Off - packet capturing is off.
- Buffer Size: 2048 KB
- Buffer used: 0 to 2048 KB

Captured packets fill the buffer up to a size of 2048 KB. While packet capturing is on, if the buffer used exceeds the stipulated buffer size, packet capturing stops automatically. In such a case, you would have to clear the buffer for further use manually.



**Note:** Packet capture details are displayed in a new window from [log viewer](#) only after enabling packet capture.



**Figure 20: Packet Capture**

### Configure

Click to configure packet capturing feature.

Capture filter can be configured through following parameters: Number of Bytes to Capture (per packet) Wrap Capture Buffer Once Full BPF String

There are various filter conditions for capturing the packets. The BPF string is used for filtering the packet capture. For example, host 192.168.1.2 and port 137.

Refer to [Configure Capture Filter](#) for more details.

## Captured Packet

The **Captured Packet** section displays a list of all captured packets. For each packet the list shows:

### Time

Packet capture time.

### In Interface

Interface from which packet is coming.

#### **Out Interface**

Interface to which packet is sent.

#### **Ethernet Type**

Ether Type: IPv4 or IPv6 or ARP

Ether Type is a field in an Ethernet frame. It is used to indicate the protocol encapsulated in the Ethernet frame.

#### **Source IP**

Source IP address (IPv4/IPv6) of the packet.

#### **Destination IP**

Destination IP address (IPv4/IPv6) of the packet.

#### **Packet Type**

Type of packet: ARP request or UDP.

#### **Ports [src, dst]**

Source and destination ports.

#### **Rule ID**

Firewall rule ID.

#### **Status**

Possible Packet Status:

- **Incoming:** Packets received on WAN or LAN interface.
- **Forwarded:** Packet forwarded to Out Interface.
- **Consumed:** Packets designated for or used by the device .
- **Generated:** Packets generated by the device.
- **Violation:** In case of any policy violation, the device will drop the packet and show the status **Violation**.

#### **Reason**

Reason for a packet being dropped, if it is dropped.

#### **Connection Status**

Displays state of connection.

#### **Served By**

Specifies if connection is Established, TIME\_WAIT or NONE.

#### **Web Filter ID**

Web filter policy ID applied on the connection traffic.

#### **Connection Flags**

System flags

#### **Application ID**

Application ID applied on the connection traffic.

#### **Application Category ID**

Application category ID applied on the connection traffic.

#### **Connection ID**

Unique ID assigned to a connection.

#### **Gateway ID**

Gateway ID through which the connection traffic is routed.

**Remote Access Policy ID**

Remote Access policy ID applied on the connection traffic.

**Bandwidth Policy ID**

Bandwidth policy ID applied on the connection traffic.

**User Group**

User group membership.

**IPS Policy ID**

IPS policy ID applied on the connection traffic.

**Application Filter ID**

Application filter policy ID applied on the connection traffic.

**Web Category ID**

Web category ID applied on the connection traffic.

**Master Connection ID**

Master connection ID of current connection.

**Username**

Name of the user establishing connection.

**Display Filter**

Click to set the filter criteria.

Packet Capture can be filtered as per the following criteria: interface name, ether type, packet type, source IP, source port, destination IP and destination port, reason, status, rule ID, user, and connection ID.

Refer to [Display Filter](#) for more details.

**Packet Information****Packet Information**

Packet information including header details and entities including firewall rules & policies.

```
Ethernet Header
Source MAC Address:12:22:5a:5b:26:a5
Destination MAC Address: 33:33:00:01:00:03
Ethernet Type IPv6 (0x86dd)
```

**Figure 21: Packet Information**

**Hex & ASCII Detail****Hex & ASCII Detail**

Packet Information in Hex & ASCII values.

```
0x0000: 6000 0000 001e 1101 fe80 0000 0000 0000 `.....'.
0x0010: bde9 2f80 d8f2 a467 ff02 0000 0000 0000 .../.g.....
0x0020: 0000 0000 0001 0003 ea53 14eb 001e aafe .....S.....
0x0030: 144d 0000 0001 0000 0000 0000 0477 7061 .M.....wpa
0x0040: 6400 0001 0001 d.....
```

**Figure 22: HEX And ASCII Details**

**Configuring Capture Filter**

The **Configuring Capture Filter** page allows configuration of number of bytes to be captured per packet.

1. Go to **Monitor & Analyze > Diagnostics > Packet Capture** and click **Configure**.

2. Enter details to configure the capture filter.

#### **Number of Bytes To Capture (Per Packet)**

Specify the number of bytes to be captured per packet.

#### **Wrap Capture Buffer Once Full**

Enable to continue capturing the packets even after the buffer is full.

When the checkbox is enabled, the packet capturing starts again from the beginning of the buffer.

#### **Enter BPF String**

Specify a BPF string.

BPF (Berkeley Packet Filter) sits between link-level driver and the user space. BPF is protocol independent and uses a filter-before-buffering approach. It includes a machine abstraction to make the filtering efficient. For example, host 192.168.1.2 and port 137.

Refer to **BPF String Parameters** for filtering specific packets.

#### **BPF String Parameters**

How to check packets of the	Example
specific host	host 10.10.10.1
specific source host	src host 10.10.10.1
specific destination host	dst host 10.10.10.1
specific network	net 10.10.10.0
specific source network	src net 10.10.10.0
specific destination network	dst net 10.10.10.0
specific port	Port 20 or port 21
specific source port	src port 21
specific destination port	dst port 21
specific host for the particular port	host 10.10.10.1 and port 21
the specific host for all the ports except SSH	host 10.10.10.1 and port not 22
specific protocol	proto ICMP, proto UDP , proto TCP

The screenshot shows the 'Configure Packet' dialog box. It contains three main sections:

- Number Of Bytes To Capture (Per Packet):** A text input field containing a placeholder '|'. This field is used to specify the number of bytes to be captured per packet.
- Wrap Capture Buffer Once Full:** A checkbox followed by a descriptive text. The checkbox is currently unchecked. The text explains that enabling it allows capturing to continue even after the buffer is full, starting again from the beginning.
- Enter BPF String:** A text input field with a placeholder 'e.g. host 192.168.1.2 and port 137'. This field is used to specify a Berkeley Packet Filter (BPF) string for filtering specific packets.

**Figure 23: Configure Packet**

3. Click Save.

## Display Filter

This page restricts the packet capturing to specific types of packets. There are further filtering conditions such as the type of interface, ether type, source IP address & destination IP Address.

1. Go to **Monitor & Analyze > Diagnostics > Packet Capture** and click **Display Filter**.
2. Enter details to configure the display filter

### Interface Name

From the list, select the physical interface used for filtering packets logs.

### Ethernet Type

Select the Ethernet type: IPv4 or IPv6 or ARP.

**Ethernet Type** is a field in an Ethernet frame. It is used to indicate the protocol encapsulated in the Ethernet frame.

### Packet Type

From the list, select the packet type used for filtering packets.

### Source IP

Specify source IP address (IPv4/IPv6).

### Source Port

Specify source port number.

### Destination IP

Specify destination IP address (IPv4/IPv6).

### Destination Port

Specify destination port number.

### Reason

Select the reason to display the filter from the available options.

#### Available

**Options:**FirewallLOCAL\_ACLDOS\_ATTACKINVALID\_TRAFFICINVALID\_FRAGMENTED\_TRAFFICICMP\_REDIRECTFILTERUSER\_IDENTITYIPSMAC\_FILTERIPMAC\_FILTERIP\_SPOOFNEIGHBOR\_POISONINGSSL\_VPN\_ACL\_

### Status

Select the status of the filter from available options.

**Available Options:**AllowedViolationConsumedGeneratedIncomingForwarded

### Rule ID

Specify ID for the rule.

### User

Select a user from the list of already existing users.

### Connection ID

Specify a connection ID.

### Clear

Click to remove the filter settings.

Interface Name	<input type="button" value="Select Interface"/>
Ethernet Type	<input type="button" value="IPv4"/>
Packet Type	<input type="button" value="None"/> <input type="button" value="HOPOPT"/> <input type="button" value="ICMP"/> <input type="button" value="IGMP"/> <input type="button" value="GGP"/> <input type="button" value="IP"/>
Source IP	<input type="text"/>
Source Port	<input type="text"/>
	<input type="text"/>
Destination Port	<input type="text"/>
Reason	<input type="button" value="Select Reason"/>
Status	<input type="button" value="Select Status"/>
Rule ID	<input type="text"/>
User	<input type="text"/>
	<input type="button" value="Add New Item"/>
Connection ID	<input type="text"/>

**Figure 24: Display Filter**

3. Click Save.

## Connection List

This page provides a current or live connection snapshot of your device in list form. Apart from the connection details, the list also provides information like firewall rule ID, user ID, and connection ID per connection. It is possible to filter the connection list as per the requirement. Click the **Connection ID** hyperlink to view the live snapshot of a specific connection in a new window.

The administrator can set the refresh interval to automatically refresh the list at the configured time interval or manually refresh the list by clicking the **Refresh** button. To filter the connection list click the **Display Filter** and specify the parameters.

### Connection List

#### Time

Connection establishment time in the format HH:MM:SS.

**Connection ID**

Unique ID assigned to a connection.

**In Interface**

Port used for the incoming connection.

**Out Interface**

Port used by the outgoing connection.

**Source IP**

Source IP address (IPV4/IPv6) of the connection.

**Destination IP**

Destination IP address (IPV4/IPv6) of the connection.

**Protocol**

Protocol used by the connection, like TCP or UDP.

**Application Name**

Name of the application that has opened the connection.

Name is displayed for the applications identified by SF-OS. If Security Heartbeat is enabled under **Protect > Advanced Threat > Security Heartbeat** then for applications that remain unidentified, **Resolve Application Info** link is displayed. Click the link to retrieve application information from the Endpoint.

If Security Heartbeat is not enabled or Endpoint devices are not connected, then **No Information Available** is displayed.

**Source Port**

Source port of the connection.

**Destination Port**

Destination port of the connection.

**Master Connection ID**

Master connection ID of the current connection.

**Rule ID**

Firewall rule ID that allows the session.

**Username**

Name of the user establishing a connection.

**Connection Status**

Displays the status of the connection.

**Flags**

System flag

**User Group**

User group membership.

**Web Filter ID**

Web filter policy ID applied on the connection traffic.

**Application Filter ID**

Application filter policy ID applied on the connection traffic.

**IPS Policy ID**

IPS policy ID applied on the connection traffic.

**Traffic Shaping Policy ID**

**QoS policy ID** applied on the connection traffic.

#### Remote Access Policy ID

Remote access policy ID applied on the connection traffic.

#### Gateway ID

Gateway ID through which the connection traffic is routed.

#### Web Category ID

Web category ID applied on the connection traffic.

#### Application ID

Application ID applied on the connection traffic.

#### Application Category ID

Application category ID applied on the connection traffic.

#### Connection Served By

Device serving the connection.

#### Translated Source

Translated source IP Address for outgoing traffic.

#### Translated Destination

Translated source IP Address for outgoing traffic.

#### Expiry (second)

Connection will expire in displayed seconds if idle.

#### Rx Bytes

The amount of data in bytes received in this session.

#### Tx Bytes

The amount of data in bytes sent in this session.

#### Rx Packets

Number of packets received in this session.

#### Tx Packets

Number of packets sent in this session.

#### Connection State

Displays state of connection.

Time	Connection ID	In Interface	Out Interface	Source IP	Destination IP	Protocol	Source Port	Destination P
15:14:43	<a href="#">23964622...</a>	PortB	-	10.200.100.13	10.200.97.205	TCP	61127	80
15:14:43	<a href="#">26207153...</a>	-	-	169.254.234.5	169.254.234.5	UDP	40043	137
15:13:30	<a href="#">31909179...</a>	-	PortB	10.200.97.205	52.26.29.75	TCP	39991	6061
15:14:44	<a href="#">24724549...</a>	-	PortA	10.198.15.35	10.198.15.255	UDP	33516	137
15:14:35	<a href="#">23964590...</a>	PortB	-	10.8.15.228	10.200.97.205	TCP	43926	80

**Figure 25: Connection List**

#### Display Filter

Use **Display Filter** page to set filtering criteria for displaying the connection list.

1. Go to **Monitor & Analyze** > **Diagnostics** > **Connection List** and click **Display Filter**.
2. Enter filter parameters

#### In Interface

Interface used by the incoming connection.

#### Out Interface

Interface used by the outgoing connection.

#### User

Name of the user establishing a connection.

#### Network Protocol

Select the network protocol used to establish a connection.

**Available Options:**IPv4IPv6

#### Source IP

IP address (IPv4/IPv6) from which the connection was established.

#### Destination IP

IP address (IPv4/IPv6) on which connection is established.

#### Packet Type

Select the type of packet used for the connection.

#### Source Port

Source port of the connection.

#### Destination Port

Destination port for the connection.

#### Rule ID

Firewall rule ID.

#### Clear

Click to remove the filter settings.

In Interface	<input type="button" value="Select Interface"/>
Out Interface	<input type="button" value="Select Interface"/>
User	
	<input type="button" value="Add New Item"/>
Network Protocol	<input type="button" value="IPv4"/>
Source IP	
Destination IP	
Packet Type	<input type="button" value="None"/> <input type="button" value="HOPOPT"/> <input type="button" value="ICMP"/> <input type="button" value="IGMP"/> <input type="button" value="GGP"/> <input type="button" value="IP"/>
Source Port	
Destination Port	
Rule ID	

**Figure 26: Display Filter**

#### Related connections

This page displays the live snapshot of the selected connection. Apart from the connection details, the list also provides information like firewall rule ID, user ID, connection ID, Web Filter ID and so on. for the selected connection.

#### Support Access

Use the Support Access page to allow Sophos Support to temporarily access your Device.

**Support Access** enables Sophos Support to connect to the Admin console of your Device without sharing the admin credentials. When the feature is enabled, an Access ID is generated using which the Support can access your device. The admin needs to convey this ID to the support.

When Support Access is enabled, Support can access your Device over HTTPS on TCP port 22 from the WAN. All connections between the Device and Support are initiated by your Device.

Specify the following:

1. Enable the Support Access on Sophos XG Firewall under **Diagnostics > Support Access** and click the toggle switch.
2. Confirm the enable message with **OK**.
3. From the drop-down menu **Grant Access for** select the time the access is valid.

4. Click **Apply** to update the settings.

5. Click **OK**.

Sophos XG Firewall establishes a secure control connection to APU (Access Proxy for UTM) and negotiates a unique access ID.

6. Communicate the **Access ID** to the support.

The support uses this access ID to login to your Device. The control connection remains established until the specified time, which is displayed next to **Access Until**.

You can disable the connection manually any time by clicking the toggle switch and confirming the disable message with **OK**.

# System

---

## Profiles

This section covers the following topics:

- **Schedule** - Schedule defines a time schedule for applying Firewall Rule or Web & Application Filter policy. This page displays a list of schedules and also provides various options to manage it.
- **Access Time** - Schedule Internet access for individual users by defining Access Time policy. This page displays list of all the default as well as custom policies.
- **Surfing Quota** - Control individual user surfing time by defining Surfing Quota policy. This page displays the list of all policies and also provides option to add, update or delete surfing quota policies.
- **Network Traffic Quota** - Limit total as well as individual upload and/or download data transfer by defining Network Traffic Quota. This page displays default as well as custom policies. The page also provides option to manage these policies.
- **Network Address Translation** - The Network Address Translation page displays list of all the NAT policies and you can sort the list based on policy name. The page also provides option to add a new policy, update the parameters of the existing policy, or delete a policy.
- **Traffic Shaping** - Traffic Shaping policy allocates & limits the maximum bandwidth usage of the user and controls the web and network traffic. This page displays list of predefined and custom policies and also provides various options to manage it.
- **Device Access** - This page shows the default and custom profiles and also provides options to manage these profiles.

## Schedule

Schedules allow you to control the time period for which firewall rules and web and application filter policies are in effect. Create schedules for specific time periods and days of the week. You can then apply these schedules to the rules and policies. A schedule also controls the system-triggered Rogue AP Scan.

Predefined and custom schedules can be applied to rules and policies. The device is shipped with the following predefined schedules:

- Work hours (5 Day week)
- Work hours (6 Day week)
- All Time on Weekdays
- All Time on Weekends
- All Time on Sunday
- All Days 10:00 to 19:00

### Types of Schedules

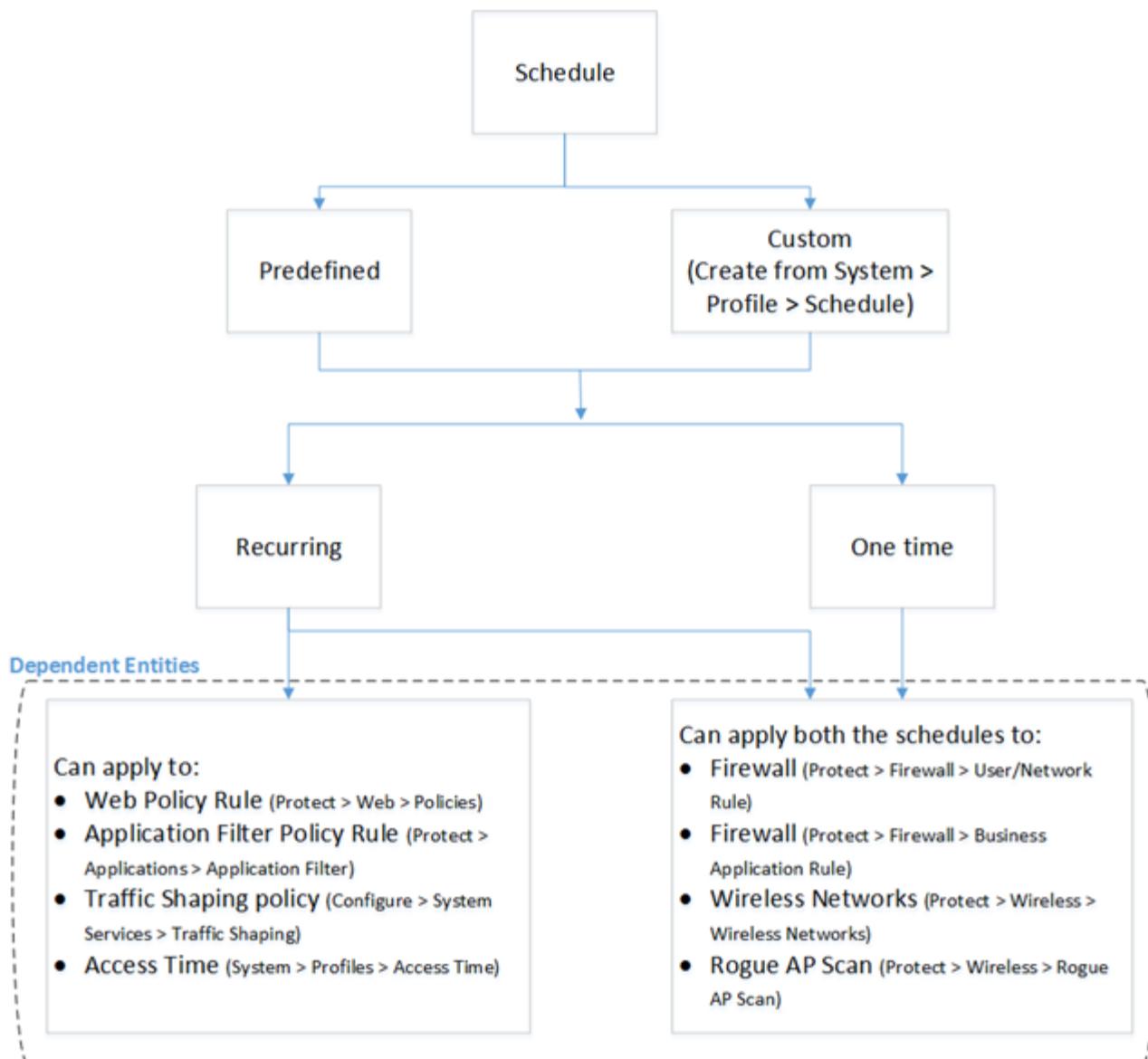
- **Recurring:** Policy recurs during the specified time periods on specified days of the week.

- **One-time:** Policy is effective once during the specified days and time period. You can apply one-time schedules to control policies related to one-time events like conferences and guest user access. One-time schedules cannot be applied to web and application policies. Hence, they are not visible on these pages.

The schedule page displays the full list of predefined and custom policies.

- You cannot delete a schedule that is currently applied to a policy. To do so, you must apply a different schedule to the policy or delete the policy itself.
- To view the policies to which a schedule is attached, to apply a schedule to a policy or to change the applied schedule, go to the corresponding policy page.
- For details of policies and rules to which the schedule can be applied, view the following diagram.

### Schedule: Basic Flow



### Add Schedule

The device allows you to add a custom schedule. This can be applied to firewall rules and web and application filter policies to specify the time period and days of the week during which they are effective.

The **Add Schedule** page allows you to add a new schedule.

1. Go to **System > Profiles > Schedule** and click **Add** on the upper right side.
2. Enter the details.

#### Name

Enter a unique name to identify the schedule.

#### Description

Enter a description for the schedule.

#### Recurrence

Click to choose the type of recurrence.

**Available Options:Recurring:** Makes the policy recur during the specified time periods on specified days of the week. Select the days of the week. Specify the start time and stop time of the schedule. Stop time cannot be earlier than the start time.**One Time:** Makes the policy effective once during the specified days and time period. You can apply it to a policy on the **Policies** page. Click on **+Add Firewall Rule** and select **User / Network Rule**. One time schedules cannot be applied to web and application policies. Hence, they are not visible on these pages.**Start Date & End Date:** (*Available only if Recurrence selected is One Time*) Select both date and time in the corresponding calendars. To specify a different start and stop time for a particular day within the range, select the day of the week from the drop-down list. Specify the start time and stop time. Stop time cannot be earlier than the start time.

The screenshot shows a configuration form for adding a new schedule. The fields are as follows:

- Name \***: A text input field labeled "Enter Schedule Name".
- Description**: A large text area for entering a description.
- Recurrence \***: A radio button group where "Recurring" is selected, and "One Time" is unselected.
- Timing \***: A section with three dropdowns: "Days" (set to "Sunday"), "Start Time" (set to "00:00"), and "Stop Time" (set to "00:00"). There is also a "+" icon for adding more rules.

**Figure 27: Add Schedule**

3. Click Save.

## Access Time

Access time enables you to Allow or Deny Internet access during a predefined time period and days of the week. While **Schedule** allows you to define the time period and the days of the week for a firewall rule or web and application filter policies, access time allows you to apply an Allow or Deny policy to the selected schedule.

Two Access Time options are available:

**Allow:** Allows access during the selected schedule

**Deny:** Denies access during the selected schedule

The device is shipped with the following predefined Access Time policies:

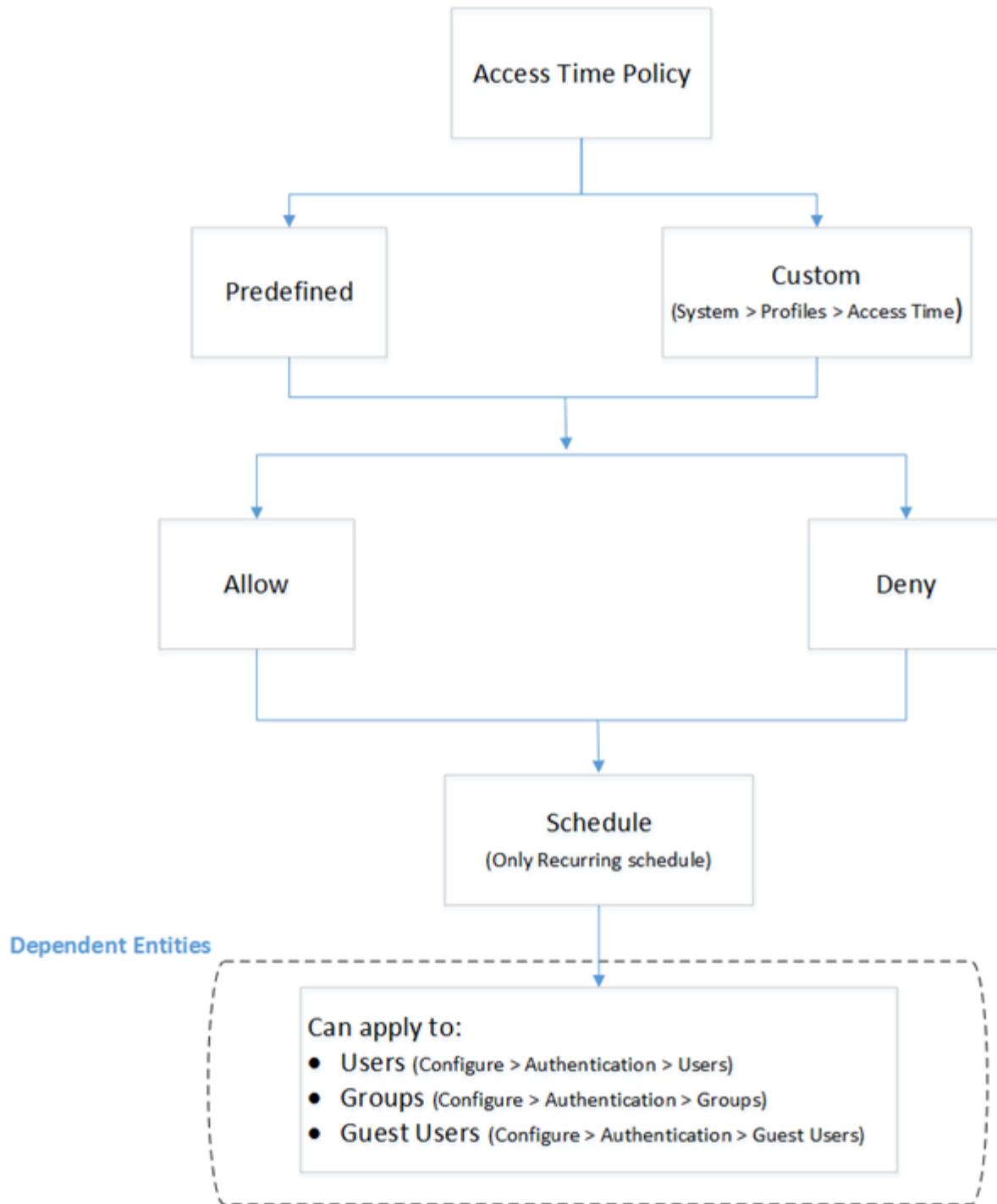
- Allowed all the time
- Denied all the time
- Allowed only during work hours (5 day week)
- Denied during work hours (5 day week)

You can create custom access time policies to define differing levels of Internet access for different users and groups based on existing schedules. The access time page displays the full list of predefined and custom policies.

**Note:**

1. You can alter only the description and schedule of an existing policy. To change the schedule of an access time policy, it is recommended that you create a new policy to ensure that the selected schedule matches the Name of the policy.
2. Access time policies can be applied only to recurring schedules. Hence, one time schedules do not appear in the drop-down list.
3. Users generally belong to a group. If the access time policy applied to the user differs from the one applied to the user's group, the user's policy takes priority.
4. For details of policies and rules to which the schedule can be applied, view the following diagram.

## Access Time Policy: Basic Flow



### Add a New Access Time Policy

To allow or deny Internet access to users or a group of users during specific time periods and days of the week, you can create access time policies. These policies are applied to existing schedules (**Profiles > Schedule**), users (**Authentication > Users**) and groups (**Authentication > Groups**). You can create custom schedules on **Profiles > Schedule**.

The **Add Access Time Policy** page allows you to add an access time policy.

1. Go to **Objects > Policies > Access Time** and click **Add** on the upper right side.
2. Enter the details.

#### Name

Enter a unique name to identify the policy.

#### Description

Enter the policy description.

#### Action

Click to choose the action to apply to the scheduled time period.

**Available Options:** **Allow:** Allows Internet access during the scheduled time period. **Deny:** Denies Internet access during the scheduled time period.

#### Schedule

Select a schedule from the available options. You can apply access time policies only to recurring schedules. Hence, one time schedules do not appear in the drop-down list.

**Available Options:** All the TimeWork hours (5 Day Week)Work hours (6 Day Week)All time on WeekdaysAll time on WeekendsAll time on Sunday

Based on the chosen **action**, Internet access is allowed or denied during the scheduled time period.



**Note:** Changes made in the access time policy become effective the instant you click Save.

**Figure 28: Add Access Time Policy**

3. Click Save.

## Surfing Quotas

Surfing quota policy allows you to assign the duration of Internet surfing time to users and groups.

- Duration of Internet access can be cyclic or non-cyclic.
- You can apply the surfing quota policy to users.

The device is shipped with the following predefined policies. Predefined policies can be applied straight away to users and groups.

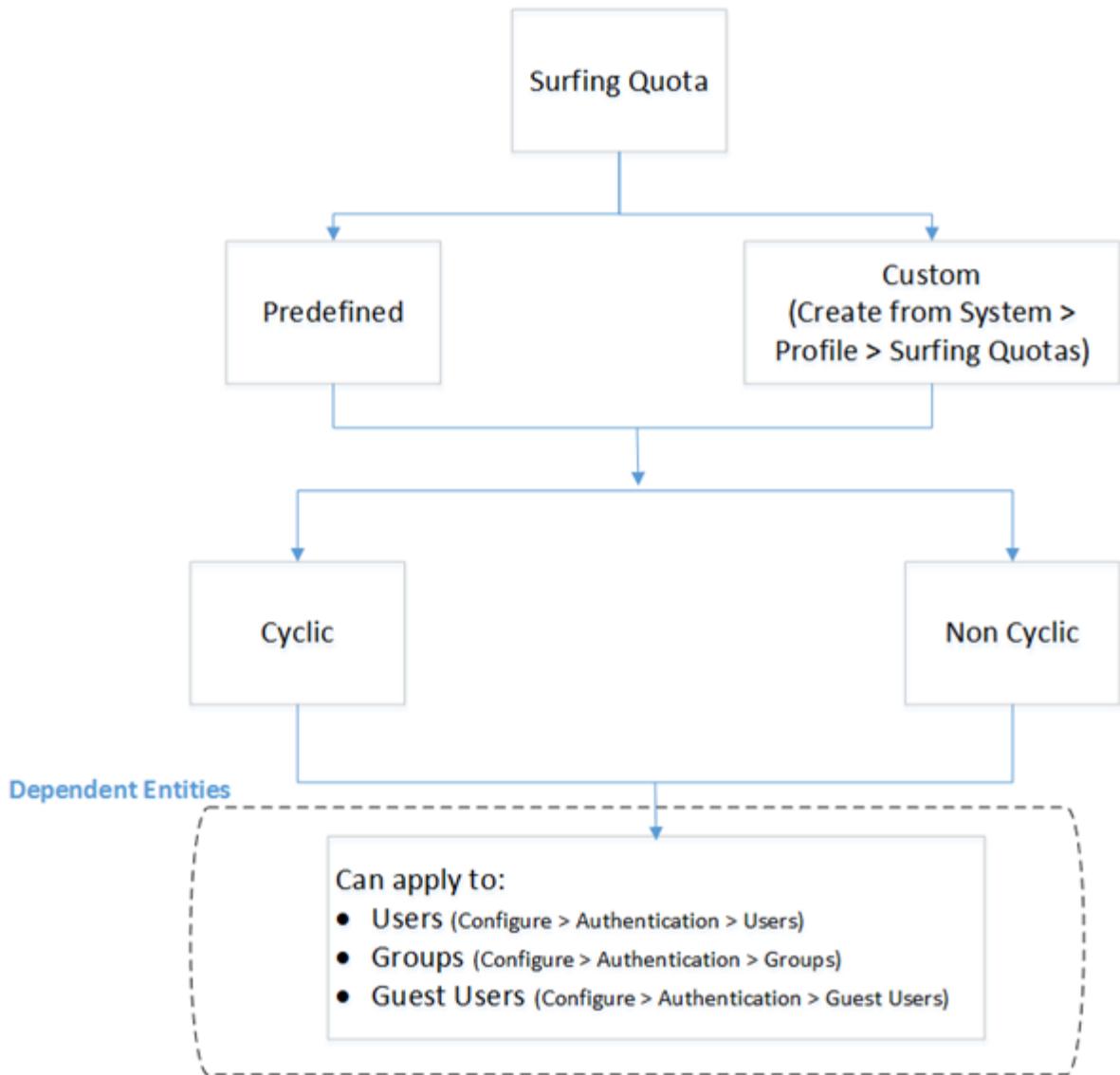
- Unlimited Internet Access
- 1 Month Unlimited Access
- 1 Month 100 hours
- Monthly 100 hours Cyclic
- Daily 1 hour Cyclic
- Weekly 7 hours Cyclic



**Note:**

1. Users generally belong to a group. If the surfing quota policy applied to the user differs from the one applied to the user's group, the user's policy takes priority.
2. For details of policies and rules to which the surfing quota policy can be applied, view the following diagram.

### Surfing Quota Policy: Basic Flow



### Add Surfing Quota

To assign the duration of Internet surfing time to users and groups, you can create surfing quota policies. These policies are then applied to users (**Configure > Authentication > Users**) and groups (**Configure > Authentication > Groups**).

The **Add Surfing Quota Policy** page allows you to create a surfing quota policy.

1. Go to **Protect > Web > Surfing Quotas** or **System > Profiles > Surfing Quotas** and click **Add** on the upper right side.

**Note:** Surfing Quota policies can also be created when applying the policy to users or groups from the respective pages. The Surfing Quota page displays the full list of predefined and custom policies.

2. Enter the details.

**Name**

Enter a unique name to identify the policy.

**Description**

Enter a description for the surfing quota policy.

**Cycle Type**

Select the cycle type.

**Available Options:** **Cyclic:** Duration of Internet access recurs for each cycle. **Non-Cyclic:** When the specified time limit ends, the user is disconnected.

**Cycle Hours (*available only if Cycle Type is Cyclic*)**

Specify the cycle hours in hours and minutes. Select the cycle from the drop-down list. Cycle hours define the upper limit of surfing hours for daily, weekly, monthly or yearly cycles.

At the end of each cycle, cycle hours are reset to zero.

Example: If cycle hours specified are 7 hours 30 minutes for a daily cycle, they are reset to zero at the end of each day whether cycle hours are fully or partially used or remain unused.

**Validity**

Select **Unlimited** if you do not want to restrict the validity period. Clear the check box to specify the validity period of Internet access.

**Maximum Hours**

Select **Unlimited** if you do not want to restrict the maximum allowed surfing duration. Clear the check box to specify the maximum duration (in hours and minutes) of surfing time allowed across the validity period.

Example: Cyclic Policy

Cycle Hours: 5 hours per day

Validity: 5 days

Maximum Hours: 20 hours

If the user accesses Internet for 5 hours each day, the user will have used 20 hours of Internet access by the end of the fourth day and hence will be disconnected.

Example: Non-Cyclic Policy

Validity: 10 days

Maximum Hours: 10 hours

The user is disconnected at the end of 10 hours even if the validity period does not expire.

The screenshot shows a configuration form for a surfing quota policy. The fields are as follows:

- Name \***: Enter Surfing Quota Policy
- Description**: Enter Description
- Cycle Type**: Cyclic (radio button selected)
- Cycle Hours \***: Hour(s) & 00 Minute(s) per Day
- Validity \***: Unlimited Day(s) (checkbox checked)
- Maximum Hours \***: Unlimited Hour(s) & 00 Minutes (checkbox checked)

**Figure 29: Add Surfing Quota Policy**

3. Click Save.

## Network Traffic Quota

The device offers two types of controls to limit bandwidth usage:

- Network Traffic Quota allows you to specify the data transfer limit. Example: User X is limited to 10 GB data transfer in a week.
- Traffic Shaping Policy (**Configure > System Services > Traffic Shaping**) allows you to control the speed of data transfer. Example: User X receives guaranteed 1 Mbps bandwidth during work hours.

Use the network traffic quota policy to specify differing types and levels of data transfer controls. Data transfer limits can be cyclic or non-cyclic. These can be based on:

- Total Data transfer (Upload + Download)
- Individual limits for Upload and Download

The device is shipped with the following predefined policies:

- 100 MB Total Data Transfer policy
- Daily 10 MB

Predefined policies are available for immediate use. You can create custom policies to specify differing data transfer limits to different users and groups.

For the policy to take effect, you must apply the network traffic quota policy to users (**Configure > Authentication > Users**) or groups (**Configure > Authentication > Groups**). Users generally belong to a group. If the network traffic quota policy applied to the user differs from the one applied to the user's group, the user's policy takes priority.

### Add Network Traffic Quota Policy

To control data transfer by users and groups, you can create network traffic quota policies. For the policy to take effect, you must then apply it to users (**Configure > Authentication > Users**) and groups (**Configure > Authentication > Groups**).

You can create the following types of policies:

- *Total Network Traffic - Cyclic Policy*
- *Total Network Traffic - Non-Cyclic Policy*
- *Individual Network Traffic - Cyclic Policy*
- *Individual Network Traffic - Non-Cyclic Policy*

1. Go to **System > Profiles > Network Traffic Quota** and click **Add** on the upper right side.
2. Enter the details.

#### Name

Enter a unique name to identify the policy.

#### Description

Enter a description for the network traffic quota policy.

#### Restriction Based On

Click to select the restriction based on the following options:

**Available Options: Total Network Traffic:** Specifies a single limit for data upload and download.

**Individual Network Traffic (Upload and Download):** Specifies different limits for data upload and download.

#### Cycle Type

Click to select the cycle type.

**Available Options:Cyclic:** Data transfer quota resets to zero at the beginning of each cycle. The user receives the full quota for each cycle. Unused quota is not carried forward to the next cycle.

**Non-Cyclic:** When data transfer reaches the specified limit, the policy expires and the user is disconnected.



**Note:** To restart the user's Internet access, go to **Configure > Authentication > Users** and **Reset User Accounting**.

3. Based on the selection made in **Restriction based on** and **Cycle Type**, you can create any one of the following four types of policies:

- a) **Policy 1: Total Network Traffic - Cyclic Policy**

#### Cycle Period

Select the cycle period from the drop-down list. Cycle period specifies the duration of cyclic policies, that is, day, week, month and year.

#### Cycle Network Traffic

Specify the network traffic limit (in MB) per cycle. It specifies the data transfer allowed during each cycle to the user. When data transfer reaches the limit, the user is disconnected.

#### Maximum Network Traffic

By default, the check box is selected to **Unlimited** and no restriction is placed on the maximum data transfer for the duration of the policy. Clear the check box to specify the maximum data transfer (in MB) allowed by the policy. When total data transfer reaches this limit, the user is disconnected.

Example: Cycle Period: Week

Cycle Network Traffic: 5 MB (5 MB data transfer is allocated to the user each week. The user is disconnected when this limit is reached during the week.)

Maximum Network Traffic: 10 MB (10 MB data transfer is allocated to the user for the duration of the policy. The user is disconnected when this limit is reached.)

The screenshot shows the configuration interface for a network traffic quota. The fields include:

- Name \***: Enter Network Traffic Quota Name (text input field)
- Description**: (text area)
- Restriction based on \***:  Total Network Traffic  Individual Network Traffic (Upload & Download)
- Cycle Type**:  Cyclic  Non-Cyclic
- Cycle Period**: Day (dropdown menu)
- Cycle Network Traffic \***: (text input field)
- Maximum Network Traffic \***:  Unlimited (checkbox) MB (text input field)

**Figure 30: Total Network Traffic - Cyclic Policy****b) Policy 2: Total Network Traffic - Non-Cyclic Policy****Maximum Network Traffic**

By default, the check box is selected to **Unlimited** and no restriction is placed on the maximum data transfer for the duration of the policy. Clear the check box to specify the maximum data transfer (in MB) allowed by the policy. When total data transfer reaches this limit, the user is disconnected.

The screenshot shows the configuration interface for a network traffic quota. The fields include:

- Name \***: Enter Network Traffic Quota Name (text input field)
- Description**: (text area)
- Restriction based on \***:  Total Network Traffic  Individual Network Traffic (Upload & Download)
- Cycle Type**:  Cyclic  Non-Cyclic
- Cycle Period**: Day (dropdown menu)
- Cycle Network Traffic \***: (text input field)
- Maximum Network Traffic \***:  Unlimited (checkbox) MB (text input field)

**Figure 31: Total Network Traffic - Non-Cyclic Policy****c) Policy 3: Individual Network Traffic - Cyclic Policy****Cycle Period**

Select the cycle period from the drop-down list. Cycle period specifies the duration of cyclic policies, that is, day, week, month and year.

**Cycle Upload Network Traffic**

By default, the check box is selected to **Unlimited** and no restriction is placed on data upload during the cycle period. Clear the check box to specify the data upload limit (in MB) per cycle. The user cannot upload data once the cycle upload network traffic reaches the limit.

**Cycle Download Network Traffic**

By default, the check box is selected to **Unlimited** and no restriction is placed on data download during the cycle period. Clear the check box to specify the data download limit (in MB) per cycle. The user cannot download data once the cycle download network traffic limit is reached.

#### Maximum Upload Network Traffic

By default, the check box is selected to **Unlimited** and no restriction is placed on data upload for the duration of the policy. Clear the check box to specify the maximum data upload allowed by the policy. The user cannot upload data once the upload network traffic limit is reached.

Example: Cycle Period: Week

Cycle Upload Network Traffic: 5 MB (5 MB data upload is allocated to the user each week. The user cannot upload data when this limit is reached during the week.)

Maximum Upload Network Traffic: 10 MB (10 MB data upload is allocated to the user for the duration of the policy. The user cannot upload data when this limit is reached.)

#### Maximum Download Network Traffic

By default, the check box is selected to **Unlimited** and no restriction is placed on data download for the duration of the policy. Clear the check box to specify the maximum data download allowed by the policy. The user cannot download data once the download network traffic limit is reached.

Example: Cycle Period: Week

Cycle Download Network Traffic: 5 MB (5 MB data download is allocated to the user each week. The user cannot download data when this limit is reached during the week.)

Maximum Download Network Traffic: 10 MB (10 MB data download is allocated to the user for the duration of the policy. The user cannot download data when this limit is reached.)

Name *	<input type="text" value="Enter Network Traffic Quota Name"/>	
Description	<input type="text"/>	
Restriction based on *	<input type="radio"/> Total Network Traffic <input checked="" type="radio"/> Individual Network Traffic (Upload & Download)	
Cycle Type	<input checked="" type="radio"/> Cyclic <input type="radio"/> Non-Cyclic	
Cycle Period	<input type="button" value="Day"/> Day <input type="button" value="Week"/> Week <input type="button" value="Month"/> Month <input type="button" value="Year"/> Year	
Cycle Upload Network Traffic *	<input checked="" type="checkbox"/> Unlimited	<input type="text"/> MB
Cycle Download Network Traffic *	<input checked="" type="checkbox"/> Unlimited	<input type="text"/> MB
Maximum Upload Network Traffic *	<input checked="" type="checkbox"/> Unlimited	<input type="text"/> MB
Maximum Download Network Traffic *	<input checked="" type="checkbox"/> Unlimited	<input type="text"/> MB

**Figure 32: Individual Network Traffic - Cyclic Policy**

d) **Policy 4: Individual Network Traffic - Non-Cyclic Policy**

#### Maximum Upload Network Traffic

By default, the check box is selected to **Unlimited** and no restriction is placed on data upload for the duration of the policy. Clear the check box to specify the maximum data upload allowed by the policy. The user cannot upload data once the upload network traffic limit is reached.

#### Maximum Download Network Traffic

By default, the check box is selected to **Unlimited** and no restriction is placed on data download for the duration of the policy. Clear the check box to specify the maximum data download allowed by the policy. The user cannot download data once the download network traffic limit is reached.

The screenshot shows a configuration form for a network traffic quota. The fields include:

- Name \***: Enter Network Traffic Quota Name (text input field)
- Description**: (text area)
- Restriction based on \***:  Total Network Traffic  Individual Network Traffic (Upload & Download)
- Cycle Type**:  Cyclic  Non-Cyclic
- Cycle Period**: Day (dropdown menu)
- Cycle Upload Network Traffic \***:  Unlimited (checkbox) [text input field] MB
- Cycle Download Network Traffic \***:  Unlimited (checkbox) [text input field] MB
- Maximum Upload Network Traffic \***:  Unlimited (checkbox) [text input field] MB
- Maximum Download Network Traffic \***:  Unlimited (checkbox) [text input field] MB

**Figure 33: Individual Network Traffic - Non-Cyclic Policy**



**Note:** Cycle Network Traffic limit cannot be greater than Maximum Network Traffic limit.

- Click Save.

## Network Address Translation

Network Address Translation (NAT) enables multiple hosts within your network to access Internet through a single public IP address. In doing so, NAT not only conserves the pool of public IP addresses, it also conceals the addressing scheme of your network.

When a client within the network sends a request to the Internet, the router forwards the request to the device. NAT translates the sender's address to the device's public IP address before forwarding the request to the Internet. When a response is received from an external source, NAT translates the public IP address into the client's private IP address before forwarding the packet to the client.

The device is shipped with a predefined NAT policy named **MASQ** which cannot be updated or deleted. The **MASQ** policy automatically masquerades traffic using the IP address that is bound to the device's WAN port.

For it to take effect, the NAT policy must be applied to a **Firewall Rule (Protect > Firewall)**. For further details, go to [User / Network Rule](#).

### Add NAT Policy

To enable internal hosts to access the Internet through a public IP address, create a Network Address Translation (NAT) policy. The policy specifies the public IP addresses through which NATing can take place. The NAT policy must then be applied to a **Firewall Rule (Protect > Firewall)**.

This page describes how to create a NAT policy.

- Go to **System > Profiles > Network Address Translation** and click **Add** on the upper right side.
- Enter the policy name.
- Select to configure the public IP address.

- IP Address: Replaces the source IP address with the configured public IP address.
  - IP Range: Replaces the source IP address with a public IP address from the specified range.
-  **Note:** To create a NAT policy for an IP address that is not bound to an interface, you must first create an interface alias. This ensures that the return traffic is routed correctly. If you want to create a NAT policy for IP address 10.10.1.30 for interface A with IP address 198.10.100.1, you must first create an alias for interface A with IP address 10.10.1.30 and then create a NAT policy for the alias.



**Figure 34: Add NAT Policy**

4. Click **Save**.

#### Related tasks

[Add Alias](#) on page 108

## Device Access

The device allows you to create role-based administrator privileges which offer granular access control. It allows you to assign some of the super administrator's capabilities to others through Device Access Profiles. You can create profiles for special-purpose administrators based on their work role. Example: Policy administration, network administration, administration of logs.

The Profiles allow three categories of access control:

- None
- Read-Only
- Read-Write

The device is shipped with the following default profiles:

- **Administrator:** Super administrator with full privileges. Administrator can create custom administrators and assign restricted or full privileges to them. Custom administrators with restricted privileges can update only their email address and password.
- **Audit Admin:** Read-write privileges only to Logs & Reports.
- **Crypto Admin:** Read-write privileges only for configuration of security certificate.
- **HAProfile:** Read-only privileges. If High Availability (HA) is configured, administrators accessing the Admin Console of the auxiliary device have the privileges that are defined in the HA Profile.
- **Security Admin:** Read-write privileges to all features, not including Profiles and Logs & Reports.



#### Note:

- You cannot modify or delete the default profiles.
- You cannot delete a profile that is currently assigned to an administrator.

## Add Profile

The device allows you to create multiple administrator profiles with differing levels of access control.

1. Go to **System > Profiles > Device Access** and click **Add**.
2. Enter the profile details.

#### Profile Name

Enter a unique name to identify the profile.

#### Configuration

Click to select the level of access to be given to a profile. You can select from the following levels of access:

**Available Options:**

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

To set a common access level for all the menus, select the options at the top (None, Read-Only or Read-Write). To set different access levels, select the option against the menu.

Click  on the left side of a menu to view the sub-menu. To set differing access levels for sub-menus, select the option against the sub-menu.

Example: If you set the access level to Read-Only against **Licensing**, the profile user can view the **Licensing** page but cannot make any modifications. To allow modifications, set the access level to Read-Write.



**Note:**

**Access Denied page**

When an administrator tries to access a page or perform an operation that is not allowed by the assigned profile, the Access Denied page is displayed.

Add Profile

Profile Name \*

Configuration	<input checked="" type="radio"/> None	<input type="radio"/> Read-Only	<input type="radio"/> Read-Write
Control Center	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Initial Setup	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
System	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Objects	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Network	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Wireless Protection	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Identity	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Security Policy	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
VPN	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
IPS	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Web & Content Filter	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Application Filter	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
WAF	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Traffic Shaping	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Email Protection	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Traffic Discovery	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Logs & Reports	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>

**Save**   **Cancel**

**Figure 35: Add Profile**

3. Click Save.

## Hosts and Services

Hosts and Services allows defining and managing system hosts and services.

This section covers the following topics:

- ***IP Host*** - The page displays the list of all dynamic and default hosts. The page also provides options to add a new host, update the existing host, or delete a host.
- ***IP Host Group*** - Host Group is a grouping of hosts. Security Policies can be created for the individual host or host groups. This page displays the list of all the host groups. It also provides options to manage these host groups.
- ***MAC Host*** - Device allows creating a host based on MAC Address. One can create a MAC Host of either a single MAC Address or multiple MAC Addresses. This page displays the list of all the available MAC host. The page also provides option to add a new MAC host, update the existing host, or delete a host.
- ***FQDN Host*** - This page displays the list of all the available FQDN host.
- ***FQDN Host Group*** - FQDN Host Group is a grouping of FQDN hosts. This page displays the list of all the available FQDN host groups.
- ***Country Group*** - Country Group is a grouping of Countries. Multiple countries can be selected to block or allow incoming traffic by using Country Group. This page displays the list of all the available Country groups.
- ***Services*** - You can use services to determine the types of traffic allowed or denied by the firewall. This page displays the list of all the default and custom services. It also provides options to manage services.
- ***Service Group*** - Service Group is a grouping of services. Custom and default services can be grouped in a single group. The page displays the list of all the default and custom groups.

## IP Host

The IP Host page displays the list of all the dynamic hosts, default hosts and manually added hosts.

Hosts allow the entities to be defined once, which can be re-used in multiple referential instances throughout the configuration. For example, consider an internal Mail Server with an IP Address 192.168.1.15. Rather than repeated use of the IP Address while configuring Security Policies or NAT Policies, it allows to create a single entity Internal Mail Server as a Host name with an IP Address 192.168.1.15. This host, Internal Mail Server can then be selected in any configuration that uses Host as a defining criterion.

By using host name instead of numerical address, 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 IP Addresses, and increases readability.

You can group multiple entities performing the same function within a single hostname.

The IP Host page displays the list of all the dynamic hosts which are automatically added on creation of VPN Remote access connections (IPsec and SSL) and the default hosts (IPv6 and IPv4) for remote access connection - ##ALL\_RW, ##WWAN1, ##ALL\_IPSEC\_RW and ##ALL\_SSLVPN\_RW along the manually added hosts. The page also provides option to add a new host, update the existing host, or delete a host.



### Note:

- System hosts cannot be updated or deleted.
- Dynamic hosts which are automatically added on creation of VPN Remote Access connections cannot be deleted.
- Default hosts (IPv6 and IPv4) for remote access connection - ##ALL\_RW, ##WWAN1, ##ALL\_IPSEC\_RW and ##ALL\_SSLVPN\_RW cannot be updated or deleted.

## Add IP Host

**Add IP Host** allows you to assign a hostname to a network, IP address, range or list.

1. Go to **System > Hosts and Services > IP Host** and click **Add**.
2. Enter the hostname.
3. Select the **IP Family**.

### Available Options:

- IPv4
  - IPv6
4. Select the host **Type**.

**Available Options:**

- IP
- Network
- IP Range
- IP List (IP addresses which belong to different networks or are not within a range.)

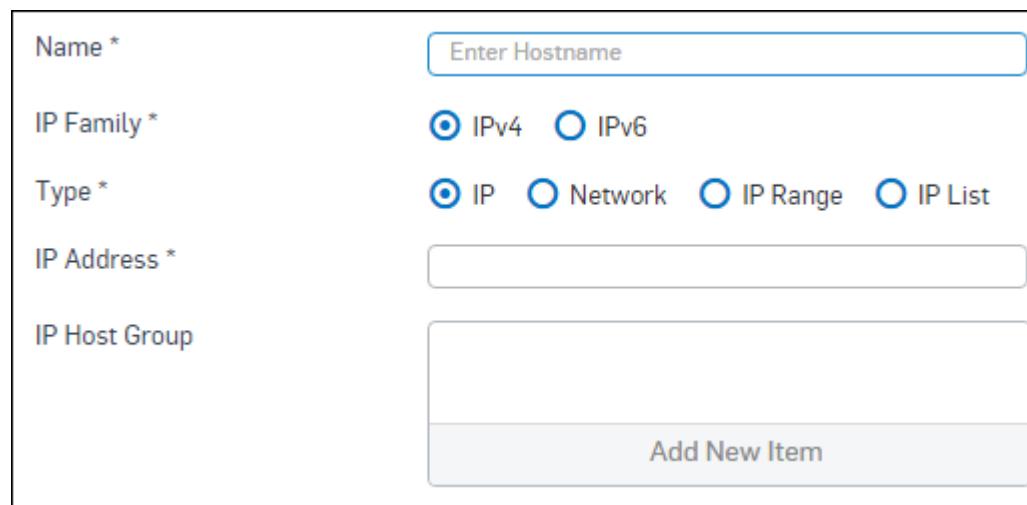
5. If the selected host type is **IP, Network or IP Range**:

1. Enter the IP address, subnet or range based on the host type.
2. Select an **IP Host Group** or create a new one.

 **Note:** A single host can be the member of multiple host groups. A host group cannot include both IPv4 and IPv6 hosts.

6. If the selected host type is **IP List**, enter the **List of IP Addresses**.

 **Note:** Only Class B IP addresses can be added to an IP list. You can add or remove an IP address from the IP list.



Name *	<input type="text" value="Enter Hostname"/>
IP Family *	<input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6
Type *	<input checked="" type="radio"/> IP <input type="radio"/> Network <input type="radio"/> IP Range <input type="radio"/> IP List
IP Address *	<input type="text"/>
IP Host Group	<input type="text"/>
<a href="#">Add New Item</a>	

**Figure 36: Add IP Host**

7. Click **Save**.

## IP Host Group

The IP Host Group page displays the list of all the host groups.

Host Group is a grouping of hosts. Security policies can be created for the individual host or host groups.

 **Note:** Dynamic host groups which are automatically added on creation of VPN Remote Access Connections cannot be deleted.

The page also provides option to add a new host group, update the parameters of the existing host group, add members to the existing host group, or delete a host group.

### Add a IP Host Group

The **Add IP Host Group** page allows you to configure an IP host group.

1. Go to **System > Hosts and Services > IP Host Group** and click **Add**.
2. Enter IP host group details.

**Name**

Enter a name to identify the IP host group.

#### Description

Enter a description for the IP host group.

#### IP Family

Select the type of IP family from the options available:

##### Available Options:

- IPv4
- IPv6

#### Select Host

The host list displays all the hosts including default hosts. Click the corresponding checkbox(es) to select the host(s). A single host can be a member of multiple host groups. A group with IPv4 and IPv6 hosts cannot be created.

The screenshot shows a configuration interface for adding an IP Host Group. It includes fields for 'Name \*' (with placeholder 'Enter Host Group Name'), 'Description' (with placeholder 'Description'), 'IP Family \*' (radio buttons for IPv4 and IPv6, with IPv4 selected), and a 'Select Host' section containing a large empty box and a 'Add New Item' button at the bottom right.

**Figure 37: Add IP Host Group**

3. Click **Save**.

The IP host group has been created and appears on the **IP Host Group** page.

## MAC Host

The device allows you to assign a hostname to one or more MAC addresses.

#### Add a MAC Host

The **Add MAC Host** page allows you to manually create a MAC Host of either a single MAC Address or multiple MAC Addresses.

1. Go to **System > Hosts and Services > MAC Host** and click **Add**.

2. Enter MAC Host details.

#### Name

Enter a name to identify a MAC Host.

#### Type

Select the MAC Host Type.

**Available Options:** **MAC Address** - Select to add a single MAC Address. **MAC List** - Select to add multiple MAC Addresses.

### MAC Address (Applicable only if Type is selected as MAC Address)

Specify MAC Address based on the Host Type selected in the form of 00:16:76:49:33:CE or 00-16-76-49-33-CE.

### List of MAC Addresses (Applicable only if Type is selected as MAC List)

Specify MAC Address based on the Host Type selected in the form of 00:16:76:49:33:CE or 00-16-76-49-33-CE.

Use comma to configure multiple MAC Addresses.

**Figure 38: Add MAC Host**

3. Click **Save**.

The MAC Host has been created and appears on the **MAC Host** page.

## FQDN Host

The FQDN Host page displays the list of all the available FQDN host.

FQDN (Fully Qualified Domain Name) Hosts allow entities to be defined once and be re-used in multiple referential instances throughout the configuration. For example, [www.example.com](http://www.example.com) has an IP Address as 192.168.1.15. Rather than remembering the IP Address of the intended website while accessing it, you can simply provide [www.example.com](http://www.example.com) in the browser. The FQDN [www.example.com](http://www.example.com) will now be mapped to its respective IP Address, and the intended webpage opens.

The page also provides option to add a new FQDN host, update the existing host, or delete a host.

### Add an FQDN Host

Use the **Add FQDN Host** page to create a new Fully Qualified Domain Name (FQDN) host.

The **Add FQDN Host** page allows you to manually configure a new FQDN host.

1. Go to **System > Hosts and Services > FQDN Host** and click **Add**.
2. Enter FQDN host details.

#### Name

Specify a name to identify the FQDN host.

#### FQDN

Specify an FQDN address. You can also specify a Wildcard FQDN by adding the prefix \*.

#### FQDN Host Group

Select an FQDN host group or add a new one. A single FQDN host can be member of multiple host groups. You can add a new FQDN host group on this page or on the **System > Hosts and Services > FQDN Host Group** page.

Name \*

FQDN \*   
Use wildcard "\*" as a prefix in FQDN to resolve sub-domains.  
For example, \*.example.com

FQDN Host Group

[Add New Item](#)

**Figure 39: Add FQDN Host**

3. Click **Save**.

## FQDN Host Group

FQDN Host Group allows you to add individual FQDN hosts to one or more host groups.

### Add FQDN Host Group

The **Add FQDN Host Group** page allows you to configure a new FQDN host group.

1. Go to **System > Hosts and Services > FQDN Host Group** and select **Add**.
2. Enter FQDN host group details.

#### Name

Enter a name to identify the FQDN host group.

#### Description

Enter a description for the FQDN host group.

#### Select Host

The host list displays all the hosts including default hosts. Click the corresponding checkbox(es) to select the host(s). A single host can be a member of multiple host groups.

Name \*

Description

Select Host

[Add New Item](#)

**Figure 40: Add FQDN Host Group**

3. Click **Save**.

## Country Group

The device offers predefined country groups based on their continent. It also offers the list of countries which appears when you create a firewall rule. You can create custom country groups.

- 💡 **Note:** On factory reset, the device resets to predefined country groups.
- 💡 **Note:** You can edit or delete predefined and custom country groups.

### Add a Country Group

The **Add Country Group** page allows you to manually configure parameters to add a new country group.

1. Go to **System > Hosts and Services > Country Group** and click **Add**.
2. Enter Country Group details.

#### Name

Enter a name to identify the Country group.

#### Description

Country Group description.

#### Select Country

Click **Add New Item** to select and add countries in the group.

A country can be a member of multiple country groups.

**Figure 41: Add Country Group**

3. Click **Save**.

## Services

The Services page displays the list of all the default and custom services.

Services are definitions of certain types of network traffic and combine information about a protocol such as TCP, ICMP or UDP as well as protocol-related options such as port numbers. You can use services to determine the types of traffic allowed or denied by the firewall.

Certain well-known traffic types have been predefined in services. These predefined services are defaults, and cannot be updated or deleted. If you require service definitions that are different from the predefined services, you can add them as custom services.

The page also provides option to add a new service, update the parameters of the existing service, or delete a service.

- 💡 **Note:**

- Service used by Security Policies cannot be deleted.
- Default Services can neither be updated nor deleted.

## Add Service

The **Add Service** page allows you to manually configure parameters to add a new Service.

1. Go to **System > Hosts and Services > Services** and click **Add**.
2. Enter Service parameters.

### Name

Enter a name to identify the Service.

### Type

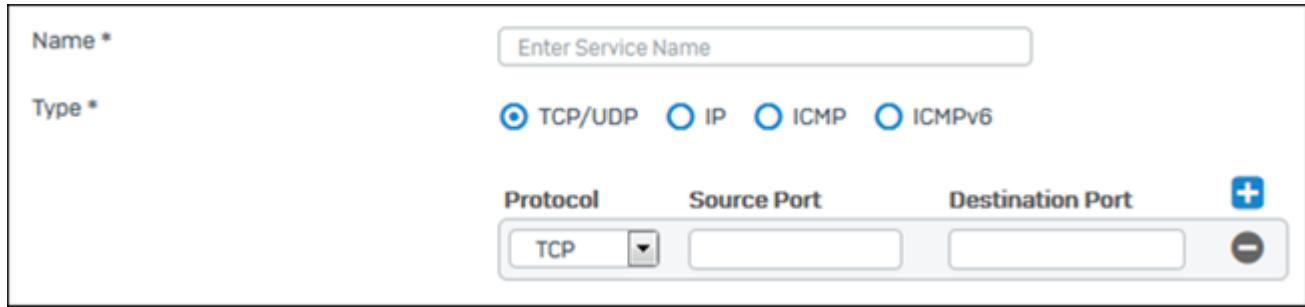
Select a protocol for the service.

**Available Options:** **TCP/UDP** - Enter Source and Destination port. You can enter multiple ports for the same service.**IP** - Select Protocol Number for the Service. You can select multiple ports for the same service.

**ICMP** - Select ICMP Type and Code. You can enter multiple types and codes for the same service. Use Add icon  and Remove icon  to add and delete the parameters respectively.

**ICMPv6** - Select ICMPv6 Type and Code. You can enter multiple types and codes for the same service.

Use Add  and Remove  to add and delete the parameters.



Protocol	Source Port	Destination Port
TCP	<input type="button" value="▼"/>	<input type="text"/> <input type="text"/>

**Figure 42: Add Service**

3. Click **Save**.

## Service Group

The Service Group page displays the list of all the default and custom service groups.

Service Group is a grouping of services. Custom and default services can be grouped in a single group.

Use to configure Security Policies to:

- block group of services for specific zone
- limit some or all users from accessing group of services
- allow only specific user to communicate using group of service

Create groups of services and then add one firewall to allow or block access for all the services in the group. A service group can contain default services as well as custom services in any combination. A single service can be a member of multiple service groups.

The page also provides option to add a new group, update the parameters of the existing group, add members to the existing group, or delete a group.



### Note:

- Default Service Groups can neither be updated nor deleted.
- Service Group used by the Security Policies cannot be deleted.

## Add a Service Group

Use the **Add Service Group** page to add a new customized Service Group.

The **Add Service Group** page allows you to manually enter details and configure a new service group.

1. Go to **System > Hosts and Services > Service Group** and click **Add**.
2. Enter Service Group details.

#### Name

Enter a name to identify the Service Group.

#### Description

Service Group Description.

#### Select Service

Service List displays all the services including default services.

Click the checkbox to select the service. All the selected services are moved to the Selected Service list.

Single service can be a member of multiple groups.

Use Search to search a service from the list.

You can create a group containing IPv4 and IPv6 services.

The screenshot shows a user interface for adding a service group. At the top left is a label 'Name \*' followed by a text input field with the placeholder 'Enter Service Group Name'. Below it is a label 'Description' followed by a text input field with the placeholder 'Description'. At the bottom left is a label 'Select Service \*' followed by a large, empty rectangular area. In the bottom right corner of this area is a light gray button labeled 'Add New Item'.

**Figure 43: Add Service Group**

3. Click **Save**.

## Administration

**Administration** allows you to manage device licenses and time, administrator access, centralized updates, network bandwidth and device monitoring and user notifications.

You can configure the following:

- *Licensing*: Synchronization and renewal of device and module subscriptions
- *Device Access*: Administrator access to device services
- *Admin Settings*: Port and login security settings for administrators
- *Central Management*: Centralized synchronization and signature updates
- *Time*: Time and date of the device
- *Notification Settings*: Mail server and email settings to send and receive alerts
- *SNMP*: Device monitoring
- *Netflow*: Network bandwidth monitoring
- *Messages*: User notifications and administrator disclaimer

## Licensing

All the modules remain unsubscribed when you deploy the device for the first time. Licensing displays the device registration information and the subscription status. You can activate or evaluate subscription modules.

Cyberoam and UTM 9 customers can migrate their licenses to SF-OS.

### Basic Information

The device offers two types of modules:

- **Basic module:** Firewall, VPN, Wireless.
- **Subscription modules:**
  - **Base Firewall** - Includes Firewall, VPN, Wireless
  - **Network Protection** - Includes Intrusion Prevention System, RED, Advanced Threat Protection
  - **Web Protection** - Includes Web Categorization, Anti Virus, Application Control
  - **Email Protection** - Includes Anti Spam, Anti Virus, Email Encryption, DLP
  - **Webserver Protection** - Includes WAF, Anti Virus, Reverse Proxy
  - **Sandstorm** - Includes the Sandstorm service and all related settings
  - **Enhanced Support** - 8 x 5
  - **Enhanced Plus Support** - 24 x 7

Once registered, the device can be used for an indefinite time period.

You can subscribe to any of the subscription modules:

- without key for free 30-days trial subscription
- with key

### Device Registration Details

#### Model

Device model number which is registered and its device key.

#### Company Name

Name of the company under which the device is registered.

#### Contact Person

Name of the contact person in the company.

#### Registered Email Address

Email address used for device registration.

#### Activate Subscription

Individual modules can be subscribed using the license key.



**Note:** **Activate Subscription** will be enabled for clicking after the original license of the device will be migrated to SF-OS from CyberoamOS or UTM 9 using **Migrate License** under **License Upgrade** section.

#### Module Subscription Details

##### Synchronize

Click to synchronize licenses with your account.

##### Activate Evaluations

Individual modules can be evaluated for the duration of 30 days.



**Note:** **Activate Evaluations** will be enabled for clicking after the original license of the device will be migrated to SF-OS from CyberoamOS or UTM 9 using **Migrate License** under **License Upgrade** section.

## Module

Name of the Module.

## Status

Indicates the status of the module.

A module can have the following status

- **Subscribed** - Module is subscribed.
- **Evaluating** - Module is subscribed under evaluation.
- **Unsubscribed** - Module is not subscribed.
- **Expired** - Subscription is expired.

## Expiration Date

Module subscription expiry date.

## License Upgrade

You can migrate licenses from CyberoamOS or UTM 9 to Sophos Firewall OS (SF-OS).

### Migrate UTM 9 License

Transfers your current UTM 9 license to an equivalent SF-OS installation. The migration is irreversible and you can no longer use this license on UTM 9.



**Note: Migrate UTM 9 License** is available only if you have migrated from UTM 9 to SF-OS.

### Migrate Cyberoam license

This option will provide you with Sophos Firewall OS license of equivalent monetary value as your Cyberoam license. All the licenses existing in Cyberoam will be migrated to SF-OS.



**Note: Migrate Cyberoam License** is available only if you have migrated from Cyberoam to SF-OS.



**Note:** Available only when device registration is complete.

## Activate Subscription

1. Go to **System > Administration > Licensing** and click **Activate Subscription** within **Device Registration Details**.
2. Enter the license key.
3. Click **Verify Key**. Subscription is activated if the license key is found valid.

## Device Access

**Device Access** allows you to limit administrative access to certain services from custom and default zones (LAN, WAN, DMZ, VPN, Wi-Fi).

1. **Local Service ACL:** The device carries a default ACL (Access Control List) when connected and powered on for the first time. Details of the default services and ports are given below. Click to enable or disable access to the services from the specified zones.

### Admin Services

LAN and Wi-Fi Zones: HTTPS (TCP port 4444), Telnet (TCP port 23) and SSH (TCP port 22)

WAN Zone: HTTPS (TCP port 443), Telnet (TCP port 23) and SSH (TCP port 22)

### Authentication Services

LAN and Wi-Fi Zones: Client Authentication (UDP port 6060), Captive Portal Authentication (TCP port 8090) and RADIUS SSO.

### Network Services

LAN, WAN, and Wi-Fi Zones: Ping/Ping6 and DNS

#### Other Services

LAN and Wi-Fi Zones: Wireless Protection, Web Proxy and SMTP relay

LAN, WAN, DMZ and Wi-Fi Zones: SSL VPN (TCP port 8443)

LAN and WAN Zones: User portal and dynamic routing

LAN, DMZ, VPN and Wi-Fi Zones: SNMP

- 💡 **Note:** User authentication services are required in order to apply user-based Internet surfing, bandwidth, and data transfer restrictions. These are not required for administrative functions.

2. **Local Service ACL Exception Rule:** You can allow access to the device's admin services from specified networks/hosts. A list of all the configured rules is displayed.

- 💡 **Note:** Once you upgrade SF-OS v15 to v16:

- If HTTP is enabled in SF-OS v15, all HTTP requests are redirected to HTTPS.
- HTTP rules in which the action is set to **Drop** are deleted.

3. **Default Admin Password Settings:**

- a) Change the default password as soon as you deploy the device.

- 💡 **Note:** The device is shipped with a default super admin with the username and password set to admin. You can access the Admin Console and CLI with these credentials. This administrator is authenticated locally by the device.

- b) Click **Reset to Default** to restore the factory default password.

Username	admin
Current Password *	<input type="password"/>
New Password *	<input type="password"/> Password
	<input type="password"/> Confirm Password
<input style="background-color: #0072bc; color: white; padding: 5px; margin-right: 10px; border-radius: 5px; font-weight: bold; width: 150px; height: 30px; border: none; font-size: 14px;" type="button" value="Apply"/> <input style="border: 1px solid #0072bc; color: #0072bc; padding: 5px; border-radius: 5px; font-weight: bold; width: 150px; height: 30px; border: none; font-size: 14px;" type="button" value="Reset To Default"/>	

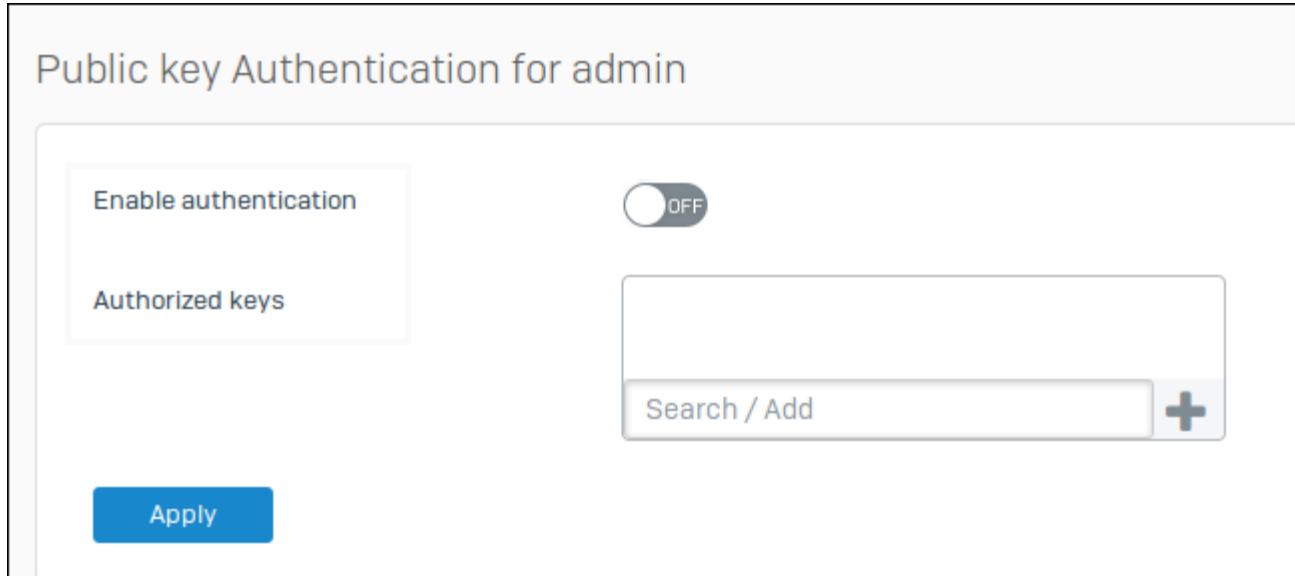
**Figure 44: Default Admin Password Settings**

4. **Public Key Authentication**

- a) Turn on **Public key authentication for admin** to allow access to the Command Line Interface (CLI) using the SSH Key.

- 💡 **Note:** Only Admin and Support users can add an SSH login key without authentication. All other users are required to provide a password for authentication before adding an SSH key.

- b) Add the list of **Authorized keys for admin**. Generate these SSH keys using SSH client tools (example: PuTTY).



**Figure 45: Public Key Authentication**

#### Related information

[Disable Telnet and HTTP behavior](#)

#### Add Local Service ACL Exception Rule

Use **Local Service ACL Exception Rule** to allow access to the device's admin services from a specified network/host.

1. Go to **System > Administration > Device Access** and click **Add** under **Local Service ACL Exception Rule**.
2. Enter a name.
3. Select the **Rule Position**.
4. Enter a description.
5. Select the **IP Family** from the following options:  
Available Options:
  - IPv4
  - IPv6
6. Select the **Source Zone** to which the rule applies.
7. Click **Add New Item** to select a host or network address to which the rule applies. Click **Create New** to create a new network/host.
8. Click **Add New Item** to select the admin **Services** to which the rule applies.  
Available Options:
  - HTTPS
  - Telnet
  - SSH
  - Web Proxy
  - DNS
  - Ping/Ping6
  - SSL VPN
  - User Portal
  - Dynamic Routing
9. Select an **Action**:

**Available Options:**

- Accept
- Drop

Rule Name \*

Rule Position

Bottom

Description

IP Family

IPv4    IPv6

Source Zone

Any

Network / Host \*

Any

Add New Item

Services \*

Add New Item

Action

Accept    Drop

**Figure 46: Add Local Service ACL Exception Rule**

10. Click Save.

## Admin Settings

**Admin Settings** allows you to modify the admin port settings and login parameters. Customize the login parameters to restrict local and remote user access based on time duration.

1. Enter host details

a) Enter a name in the form of a Fully Qualified Domain Name (FQDN).

Acceptable Range: 0 to 256 characters

Example: security.sophos.com



**Note:** When the device is deployed for the first time, the serial ID of the device is saved as the hostname.

b) Enter the description.

Hostname  
Description  
Apply

**Figure 47: Hostname**

## 2. Configure Admin Port settings

- a) Displays the HTTP port configured in SF-OS v15 if you have upgraded from SF-OS v15 and enabled HTTP service.

Default: 80

**Note:** From v16 onwards, the device does not support access of Admin console on this port. Traffic on HTTP port is automatically redirected to HTTPS port.

- b) Enter the port number to configure the HTTPS port for secure Admin Console access.

Default: 4444

- c) Enter the port number to configure the HTTPS port for secure User Portal access.

Default: 443

- d) Select the **Certificate** to be used by User Portal, Captive Portal, SPX Registration Portal and SPX Reply Portal.

Admin Console HTTPS Port \* 4444  
User Portal HTTPS Port \* 443  
Certificate \* ApplianceCertificate (Selected certificate will be used for My Account, Captive Portal, SPX Registration Portal & Reply Portal)  
Apply

**Figure 48: Admin Port Settings**

## 3. Set login security for Administrators

- a) Select the checkbox and configure the duration (in minutes) of inactivity for the administrative session after which the device is locked automatically. This configuration is applicable to Admin and CLI Console, IPsec Connection Wizard, Network Wizard, Group Import Wizard.

Default: 3 minutes

- b) Select the checkbox and configure the period (in minutes) of inactivity after which the administrator is logged out automatically.

Default: 10 minutes

**Note:** The Logout Admin Session After value must be greater than the Lock Admin Session After value.

- c) Select the checkbox to block login to the Admin Console and CLI. Enter the maximum number of failed login attempts and the duration (in seconds) within which the attempts can be made from a single IP address. When the failed attempts exceed the number, the administrator is locked. Specify the number of minutes for which the administrator will not be allowed to login. The administrator account will be locked for the configured minutes if the allowed failed login attempts exceeds.

The screenshot shows a configuration panel for login security. It includes the following settings:

- Lock Admin Session After  Minutes Of Inactivity
- Logout Admin Session After  Minutes Of Inactivity
- Block Admin Login
- After  unsuccessful attempts from same IP in  Seconds (1-120)
- Block login access for  Minutes (1-60)

**Figure 49: Login Security Settings**

4. Select the checkbox to enable password complexity settings for Administrators and enforce the required constraints.

The screenshot shows a configuration panel for administrator password complexity. It includes the following settings:

- Enable Password Complexity Check
  - Minimum Password length should be of  characters
  - Include at least 1 upper-case and 1 lower-case alphabetic character
  - Include at least 1 numeric character
  - Include at least 1 special character like '@', '\$', '!', etc

( Note: Password must not be a username )

**Figure 50: Administrator Password Complexity Settings**

5. Select **Enable Login Disclaimer** to set messages for authentication, SMTP, administration and SMS customization, which administrators must agree to before they can log in to the Admin Console and CLI. You can customize and preview messages too.

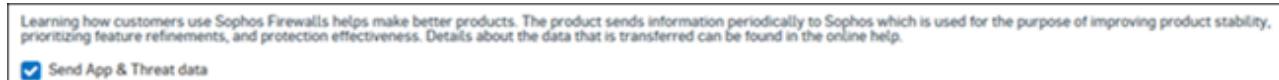
The screenshot shows a configuration panel for login disclaimer. It includes the following settings:

- Enable Login Disclaimer
  - [Click Here](#) to modify the disclaimer message ( System > Administration > Messages )
  - [Click Here](#) to preview the disclaimer message

**Figure 51: Login Disclaimer Settings**

6. Select **Sophos Adaptive Learning** to send the following application usage and threat data to Sophos: Unclassified applications (to improve network visibility and enlarge the application control library), Data for IPS alerts, detected virus (including URLs), spam, ATP threats such as threat name, threat URL/IP, source IP, and applications used.

The device sends periodic information to Sophos over HTTPS to improve stability, prioritize feature refinements, and to improve protection effectiveness. No user-specific information or personalized information is collected. The device sends configuration and usage data by default. This includes device information (example: model, hardware version, vendor), firmware version and license information (does not include owner information), features that are in use (status, on/off, count, HA status, central management status), configured objects (example: count of hosts, policies), product errors, and CPU, memory and disk usage (in percentage).



**Figure 52: Sophos Adaptive Learning**

## Central Management

Sophos Firewall Manager (Firewall Manager) centrally manages your Sophos Firewall (device). Central Management allows you to configure keep-alive requests and to enable configuration and signature updates of the device through the Firewall Manager.

1. Go to **System > Administration > Central Management**.
2. Turn on **Manage your firewall using**.
3. Choose **Sophos Firewall Manager (SFM)** or **Sophos Central Firewall Manager (CFM)** to manage your firewall.

### Sophos Firewall Manager

1. Select **Device Management** to send keep-alive requests and check for configuration updates.
2. Under **Advanced Settings**:
  1. Select the communication settings from the following options:
 

**Available Options:**

    - Firewall Manager will push configuration changes to the Firewall Device
    - Firewall Device will fetch configuration changes from the Firewall Manager
  2. Enter the **HTTPS Port on Firewall Manager** over which configuration updates are to be sent.  
Default: 443
  3. Select **Communication Heartbeat Protocol** to define how keep-alive information is sent to the Firewall Manager.
 

 **Note:** We recommend that you set the Heartbeat protocol to Syslog.
  3. Enable **Update Management** to receive signature updates from the Firewall Manager.
  4. Under **Advanced Settings**:
    1. Enter the **Firewall Manager Port** over which the Firewall Manager pushes signature updates.  
Default: 8443
    -  **Note:** Enter the same port number that is configured in **Administration Settings** of the Firewall Manager.

**Central Management Settings**

Manage your firewall using

Sophos Firewall Manager (SFM)

Firewall Manager IP Address/Domain \*

Sophos Central Firewall Manager (CFM)

CFM is managed by your Sophos Partner

Device Management

Select this option to set the method of applying configuration changes and to choose the communication protocol between the central management server and managed firewalls. Firewall will fetch the configuration from the Firewall Manager based on the current settings.

Advanced Settings

Firewall Manager will **push** configuration changes to the firewall.  
Select this option if the firewall is directly reachable from the Firewall Manager.

Device will **fetch** configuration changes from the Firewall Manager. HTTPS Port on Firewall Manager   
Select this option if the firewall is behind a NAT device. The firewall checks for configuration changes at regular intervals.

Communication Heartbeat Protocol  Syslog (Port 6514)  HTTPS Port

Update Management

Choose this option to instruct the firewall to check for firmware and pattern updates from the Firewall Manager, instead of checking the Up2date service.

Advanced Settings

Firewall Manager Port \*

## Sophos Central Firewall Manager

1. In **Device Management**
2. Under **Advanced Settings**:

1. Select the communication settings from the following options:

**Available Options:**

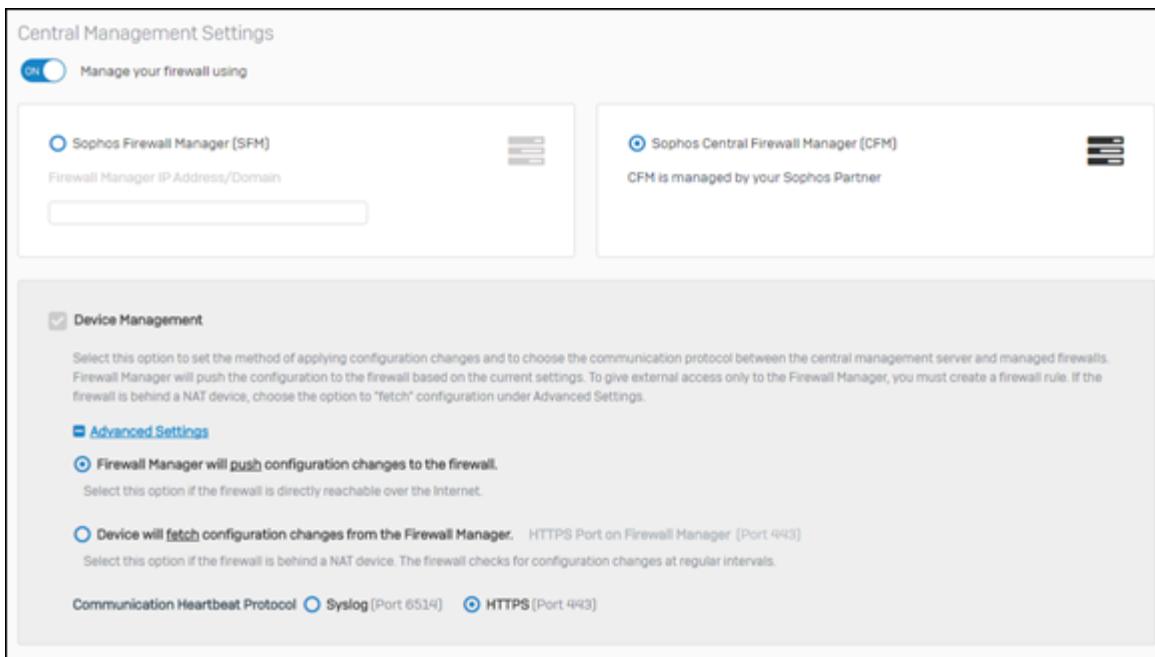
- Firewall Manager will push configuration changes to the Firewall Device
- Firewall Device will fetch configuration changes from the Firewall Manager

2. Enter the **HTTPS Port on Firewall Manager** over which configuration updates are to be sent.

Default: 443

3. Select **Communication Heartbeat Protocol** to define how keep-alive information is sent to the Firewall Manager.

 **Note:** We recommend that you set the Heartbeat protocol to Syslog.



Restrictions apply if you are managing SFOS V16 devices from SFM V15. For details refer to [Appendix F - Compatibility with SFMOS 15.01.0](#)

## Time

You can set the time and date to the device's clock or synchronize the device with a Network Time Protocol (NTP) server.

1. Go to **System > Administration > Time**.
2. **Current Time** displays the device time and date.
3. Select the **Time Zone** based on the location in which the device is deployed.
4. Select from the following options to choose how you set the time and date:
  - **Use pre-defined NTP server** (pool.ntp.org). The device uses NTP version 3 (RFC 1305). Click to **Sync Now**.
  - **Use Custom NTP server**. Enter the IPv4 address or IPv6 address or domain name. You can configure up to 10 NTP servers. At the time of synchronization, the device queries the configured NTP servers sequentially until it receives a valid reply from a server. Click to **Sync Now**.
  - Select **Do not use NTP Server** to configure the date and time based on the device's clock. Set the date and time.

Current Time: 2015-10-21 14:51:04

Time Zone: Asia/Kolkata

Use pre-defined NTP Server

Use Custom NTP Server

(Enter NTP Server IP Address/Domain)

Do not use NTP Server

Date: 10/21/2015

Time: 14 HH 51 MM 04 SS

**Figure 53: Setting Device's Date and Time**

## Notification Settings

Notification Settings allows you to configure the mail server IP address, port, and email address to send and receive alert emails.

The device allows you to configure email notifications for system-generated events and reports to inform the administrator about:

- Change in gateway status
- Change in HA (high availability) link status (if HA cluster is configured)
- Change in the state of IPsec tunnels

### 1. Mail Server Settings

Click to Send Notifications Via:

#### Built-in Email Server

Select if you want to use the built-in Email Server in the Device to send system-generated emails.

#### External Email Server

Select to configure an External Email Server to send system-generated emails.

1. Specify the **Mail Server IPv4 Address or FQDN Address and Port Number**. Default Port: 25
2. Select **Authentication Required** to authenticate the user before sending an email. Specify **Username** and **Password**.
3. Select **Connection Security** mode to be used for establishing a secured connection between an SMTP client and the SMTP server for SMTP mail notification. Available Options:

- None
- STARTTLS
- SSL/TLS

Default: **None**

4. Select a **Certificate** to be used for authentication by the SMTP client and the SMTP server.

Default: ApplicationCertificate

Mail Server IPv4 Address/FQDN \* - Port \*

- 25 Default - 25

Authentication Required

Username

Password  \*\*\*\*\*

Connection Security \*

Certificate

**Figure 54: Mail Server Settings**

## 2. Email Settings

Enter the sender and recipient email addresses.

From Email Address \*

Send Notifications to Email Address \*

**Figure 55: Email Settings**

## 3. Email Notification

Select **IPsec Tunnel UP/Down** to enable receipt of email notifications if IPsec VPN tunnel connectivity is lost.

Email alerts are sent to the configured email address.

An email is sent only when Host-to-Host and Site-to-Site tunnel connections are disconnected for one of the following reasons:

- A peer is found dead (DPD)
- Failed to re-establish connection after Dead Peer Detection (DPD)
- IPsec Security Association (SA) is expired and is required to be re-established.
- IPsec tunnel comes up without administrator intervention after losing the connectivity.



### Note:

- An email is sent for each subnet pair in case of Site-to-Site connections with multiple local/remote networks.
- Description of IPsec tunnel connection is included in the email only if the administrator has provided the information.

IPsec Tunnel Up/Down  Enable

**Figure 56: The email contains the following Notification**

## 4. Test Mail

Click to preview and edit the email address details.

Click **Send**.



**Note:** Mail server configuration changes automatically when the changes are made from the Network Configuration Wizard and vice versa.

## SNMP

**SNMP** (Simple Network Management Protocol) allows you to configure the Sophos Firewall device as an SNMP agent. The device responds to multiple SNMP managers within the predefined communities. You can monitor multiple firewall devices on IP networks for device availability, CPU, memory and disk utilization, availability of critical services and more. The device stores information in a Management Information Base (MIB) and replies to SNMP Get commands for MIB. Click [here](#) to download the Sophos MIB file. It also sends SNMP traps (alerts) to the SNMP manager.

SNMP collects information in two ways:

- SNMP manager polls the agents.
- Agents send traps to the SNMP manager.

**SNMP Community** consists of a manager and a group of agents. Agents can belong to more than one SNMP community. The community defines where information is sent. An agent does not respond to requests from managers that do not belong to its communities. You must specify a trap version for each community. Each community can support SNMPv1 and SNMPv2c. Sophos Firewall device supports IPv4 and IPv6 addresses.

**Agent Configuration** allows you to configure the agent details.

**Community** displays a list of all the communities. You can sort, add, update, or delete communities.

### SNMP Agent Configuration

**SNMP Agent Configuration** allows you to configure the device as an SNMP agent.

1. Go to **System > Administration > SNMP**.
2. Select to enable the SNMP Agent.
3. Enter a name.
4. Enter the description.
5. Enter the physical location of the device.
6. Enter the contact information of the person responsible for maintaining the device.
7. The **Agent Port** uses UDP port 161. This port receives GET requests from the SNMP managers.
8. Specify the **Manager Port** over which the SNMP manager receives alerts/traps from the SNMP agent.

Default: 162

Enable SNMP Agent

Name \*

Description

Location \*

Contact Person \*

Agent Port \* 161

Manager Port \* 162

**Apply**

**Figure 57: Agent Configuration****Add Community**

1. Go to System > Administration > SNMP and click Add.
2. Enter a name.
3. Enter the description.
4. Enter the IP address (IPv4/IPv6) of the SNMP manager.
5. Select the SNMP protocol version. SNMP v1 and v2c-compliant SNMP managers have read-only access to device system information and can receive device traps.
6. Select the version for trap support. Traps are sent only to SNMP managers that support the specified versions.
7. Click Save.

Name \*

Description

IP Address \*

Protocol Version \*

v1  v2c

Trap Support

v1  v2c

**Figure 58: Add SNMP Community**

## Netflow

**Netflow** allows you to add, update, or delete Netflow servers. The device offers Netflow, a network protocol, to monitor network bandwidth usage and traffic flow. Netflow records of source, destination and volume of traffic are exported to the Netflow server. The records help you identify the protocols, policies, interfaces and users consuming high bandwidth. Data analyzing tools like Open Source Data Analyzer and PRTG software can generate reports from the Netflow records.

### Netflow Configuration

1. Enter the **Netflow Server Name**.
2. Enter the **Netflow Server IP/Domain**. You can enter IPv4 or IPv6 addresses.
3. Enter the **Netflow Server Port** number (UDP port). Records are sent to the Netflow server over the specified port.

Default: 2055

Server Name	Netflow Server IP/Domain	Netflow Server Port		
<input type="text"/>	<input type="text"/>	2055		

**Figure 59: Netflow**

-  **Note:** Traffic of only those firewall rules that have **Log Firewall Traffic** enabled is sent to the Netflow server.
-  **Note:** You can configure up to five Netflow servers.
-  **Note:** Sophos supports Netflow v5. You can export all the parameters of v5.

## Messages

Use Messages to notify users and issue administrative alerts.

You can send messages of up to 256 characters to a single user or multiple users simultaneously.

You can send notifications related to the following events:

- Authentication: Login and logout confirmation, login failure and disconnection
- SMTP: Blocked and received emails
- Administration: Disclaimer for admin login
- SMS Customization: Login information to guest users

## Certificates

Certificates allows you to add certificates, certificate authorities and certificate revocation lists.

- [Certificates](#)
- [Certificate Authorities](#)
- [Certificate Revocation Lists](#)

## Certificates

Digital certificates provide verification of ownership of a user or computer (example: VPN) or an organization (example: websites) over the Internet, and are issued by a Certificate Authority (CA). Certificate Signing Requests (CSR) enable you to provide the information required for the CA to issue a certificate. CAs issue certificates

which can include the owner's public key, the certificate's validity period, owner information and the private key. Verification is completed through the private key which is held by the owner.

Certificates are revoked when the private key is lost, stolen or updated. CAs maintain a list of valid and revoked certificates. Self-signed certificates that are revoked are automatically added to the Certification Revocation List (CRL).

The device allows you to:

- generate a self-signed certificate, upload a third-party certificate, or to generate a CSR.
- use the device as the CA or add an external CA.
- revoke a self-signed certificate or upload an external CRL.

### Add Certificate

**Add Certificate** allows you to upload a certificate, generate a self-signed certificate, or to generate a Certificate Signing Request (CSR).

1. Go to **System > Certificates > Certificates** and click **Add**.
2. Select from the following options.

*[Upload Certificate](#)*

*[Generate self-signed Certificate](#)*

*[Generate Certificate Signing Request](#)*

### Upload Certificate

1. Enter the **Certificate Name**.
2. Select the format of certificate file.

**PEM (.pem)**: Base64 encoded form of DER certificate. Certificate and private key are stored in different files.

**DER (.der)**: Binary form of PEM certificate used on Java platform. Certificate and private key are stored in different files.

**PEM (.pem)**: Base64 encoded form of DER certificate. Certificate and private key are stored in different files.

**DER (.der)**: Binary form of PEM certificate used on Java platform. Certificate and private key are stored in different files.

**CER (.cer)**: Binary form. Contains certificate owner information and public and private keys.

**PKCS7 (.p7b)**: ASCII code. Contains the certificate but not the private key.

**PKCS12 (.pfx or .p12)**: Binary form used on Windows platforms. Stores the private key with the public key.

3. Upload certificate and private key.
4. Enter the CA passphrase and re-enter to confirm.
5. Click **Save**.

### Generate Self-Signed Certificate

1. Go to **System > Certificates > Certificates** and click **Add**.

2. Set **Action** to **Generate self-signed certificate**.

3. **Ceritificate Details**

- a) Enter the **Certificate Name**.

- b) Specify the certificate's validity period.

Default: 1 day

- c) Select the number of bits used to construct the key from the list.



**Note:** Larger keys offer greater security, but take longer to encrypt and decrypt data.

Default: 2048

- d) Select to encrypt the key. Enter a passphrase or the pre-shared key and re-confirm
- e) Specify the certificate ID for one of the following options:
  - DNS
  - IP Address (IPv4/IPv6 Address)
  - Email
  - DER ASN1 DN (X.509)

#### 4. Identification Attributes

- a) Select the country in which the device is deployed.
- b) Enter the state within the country.
- c) Enter the locality in which the certificate is to be used.
- d) Enter the name of the certificate owner (example: Sophos Group).
- e) Enter the name of the department to which the certificate is to be assigned (example: marketing).
- f) Enter the common name or FQDN (example: marketing.sophos.com).
- g) Enter the contact person's email address.

### 5.

#### Generate Certificate Signing Request

The device allows you to generate a Certificate Signing Request (CSR) which can be sent to a CA.

1. Go to **System > Certificates** and click **Add**.
2. Set **Action** to **Generate Certificate Signing Request (CSR)**.

#### 3. Ceritificate Details

- a) Enter the **Certificate Name**.
- b) Specify the certificate's validity period.  
Default: 1 day
- c) Select the number of bits used to construct the key from the list.



**Note:** Larger keys offer greater security, but take longer to encrypt and decrypt data.

Default: 2048

- d) Select to encrypt the key. Enter a passphrase or the pre-shared key and re-confirm
- e) Specify the certificate ID for one of the following options:
  - DNS
  - IP Address (IPv4/IPv6 Address)
  - Email
  - DER ASN1 DN (X.509)

#### 4. Identification Attributes

- a) Select the country in which the device is deployed.
- b) Enter the state within the country.
- c) Enter the locality in which the certificate is to be used.
- d) Enter the name of the certificate owner (example: Sophos Group).
- e) Enter the name of the department to which the certificate is to be assigned (example: marketing).
- f) Enter the common name or FQDN (example: marketing.sophos.com).
- g) Enter the contact person's email address.

#### 5. Click Save.

Once the certificate is created, you need to download and send this certificate to the remote peer with whom the connection is to be established.

## Download Certificate

The device allows you to download self-signed certificates and certificate signing requests.

1. Go to **System > Certificates > Certificates**.
2. Go to the **Manage** column and click  against the certificate. The certificate is downloaded as a .tar.gz file.

## Revoke Certificate

1. Go to **System > Certificates > Certificates**.
2. Go to the **Manage** column and click  against the certificate. You can revoke lost, stolen or updated self-signed certificates.

Revoked certificates are automatically added to the Certificate Revocation List (CRL).

## Certificate Authorities

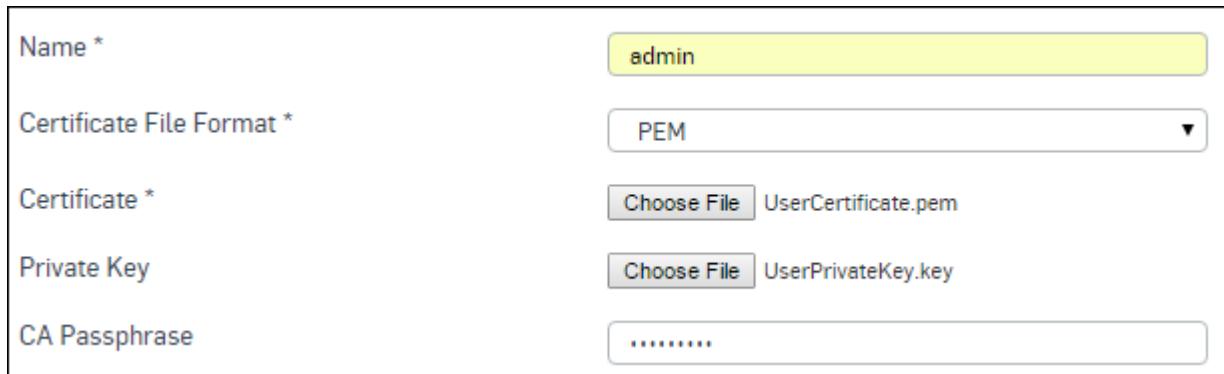
Certificate Authorities (CA) are trusted entities which issue digital certificates that verify the ownership of a user, host or organization. Ownership is verified through a public key, owner information and a private key.

The device allows you to generate a local CA or to import external CAs. Among external CAs, it provides Verisign, Entrust and Microsoft.

The default CA is regenerated automatically when it is updated.

### Add Certificate Authority

1. Go to **System > Certificates > Certificate Authorities** and click **Add**.
2. Enter the name of the CA.
3. Select the format of the root certificate. The certificate and private key are stored in different files.
4. Upload the certificate and private key.
5. Enter the CA passphrase and re-enter to confirm.



Name *	<input type="text" value="admin"/>
Certificate File Format *	<input type="text" value="PEM"/>
Certificate *	<input type="button" value="Choose File"/> UserCertificate.pem
Private Key	<input type="button" value="Choose File"/> UserPrivateKey.key
CA Passphrase	*****

**Figure 60: Add Certificate Authority**

6. Click **Save**.

## Download CA

You can download local CAs in order to forward these to the remote peer for the verification process.

1. Go to **System > Certificates > Certificate Authorities**.
2. Click  to download the zip file.

## Update Default CA

**Edit Default CA Parameters** allows you to edit the default certificate authority details.

1. Go to **System > Certificates > Certificate Authorities**.
2. Go to the **Manage** column and click  against the default certificate.
3. The name of the CA cannot be changed for default CA.
4. Select the country in which the device is deployed.
5. Enter the state within the country.
6. Enter the locality in which the certificate is to be used.
7. Enter the name of the certificate owner (example: Sophos Group).
8. Enter the name of the department to which the certificate is to be assigned (example: marketing).
9. Enter the common name or FQDN (example: marketing.sophos.com).
10. Enter the contact person's email address.
11. Enter the CA passphrase and re-enter to confirm.
12. Click **Save**.

## Regenerate Certificate Authority

1. Go to **System > Certificates > Certificate Authorities**.
  2. To regenerate the default certificate, go to the **Manage** column and click .
-  **Note:** When you update the default CA, it is automatically regenerated.

## Certificate Revocation Lists

Certificates can be revoked when the key or CA has been compromised, or the certificate is no longer valid for the original purpose. CAs maintain a list of revoked certificates.

You can upload Certificate Revocation List (CRL) of an external CA. Self-signed certificates that are revoked are automatically added to the CRL.

### Add CRL

**Add CRL** allows you to upload the Certificate Revocation List (CRL) of an external certificate authority.

1. Go to **System > Certificates > Certificate Revocation Lists** and click **Add**.
2. Enter the **CRL Name** and upload the CRL file.
3. Click **Save**.

### Download CRL

When you add a CA, a default CRL file **default.tar.gz**, is generated.

1. Go to **System > Certificates > Certificate Revocation Lists**.
2. Click **Download** against the CRL to download the .zip file.

## Backup & Firmware

---

Backup & Firmware provides following options:

- ***Backup & Restore*** : Backup and restore system data.
- ***API***: Application Programming Interface (API) allows third party applications to communicate with the device.
- ***Import Export*** : Import/export device configuration from/to a text file.
- ***Firmware***: Allows you to upload/view firmware versions downloaded.

- *Pattern Updates* : Update patterns for various modules like Sophos AV, IPS, WAF or set auto-update interval.

## Backup & Firmware

Backup is the essential part of data protection. No matter how well your system is treated, no matter how much it is taken care of, you cannot guarantee that your data is safe, if it exists only at one place.

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

Backup consists of all the policies and all other user related information.

Device facilitates to take back-up only of the system data, either through scheduled automatic backup or using a manual backup.

Once the backup is taken, the file for restoring the backup must be uploaded for restoring the configuration.

Below are the screen elements with their description:

### **Backup**

#### **Backup Mode**

Select how and to whom backup files should be sent.

#### **Available Options:**

**Local** - Backup is taken and stored on the Device itself.**FTP** - Configure FTP server IP Address (IPv4/IPv6), login credentials and FTP path. **Email** - Configure Email Address on which backup is to be mailed. You can configure multiple Email Addresses.

#### **Backup Prefix**

Specify backup file name (prefix). The backup file name format is as follows:

- With Prefix: <Prefix>\_Backup\_<Device Key>\_<timestamp>

For example:

Dallas\_Backup\_ABCDEY190\_26Nov2014\_12.09.24

NY\_Backup\_ABCDEY190\_26Nov2014\_12.09.24

- Without Prefix(Default): Backup\_<Device Key>\_<timestamp>

For example:

Backup\_ABCDEY190\_26Nov2014\_12.09.24

If prefix is not provided, the default format is used for backup file.

Backup Prefix will be useful in case you need to take backup from multiple devices.

#### **Frequency**

Select the system data backup frequency.

In general, it is best to schedule backup on regular basis. Schedule can be determined depending on how much information is added or modified.

#### **Available Options:**

**Never** - Backup will not be taken at all **Daily** - Backup will be taken every day **Weekly** - Backup will be taken every week **Monthly** - Backup will be taken every month

#### **Schedule**

Specify the day/date and time for Daily, Weekly and Monthly backup.

#### **Backup Now**

Click to take the backup of system data till date.

**Download (Only for Local Backup Mode)**

Click to download the latest backup that is available for uploading.

Backup Mode:  Local  FTP  Email

Backup Prefix:

Frequency:  Never  Daily  Weekly  Monthly

**Apply** **Backup Now**

**Figure 61: Backup****Backup Restore****Restore Configuration**

To select the complete path of the backup file to be restored, click the file selection button against **Restore Configuration**.

**Upload and Restore**

Click to upload and restore the configuration.

Restore Configuration  No file selected.

**Upload and Restore**

**Figure 62: Backup Restore**

**Note:** Restoring data older than the current data results in the loss of current data.

**API**

Application Programming Interface (API) is an interface which allows third party applications to communicate with the device. This page allows the Administrator to log on and log off users.

**API Configuration****API Configuration**

Enable to allow only authorized third-party solution providers like ISP, and system integrators to use API for log-on and log-off process.

Default - Disabled

**Allowed IP Address**

Add the IP addresses allowed to place the XML log-on and log-off requests.

You will be able to add IP Address only if API Configuration is enabled.

The screenshot shows a configuration interface for 'API Configuration'. At the top right is a checkbox labeled 'Enabled' which is checked. Below it is a large input field with a 'Search / Add' button and a '+' icon. The entire interface is contained within a light gray border.

**Figure 63: API Configuration**

### API Explorer

#### Request XML String

Specify the XML content containing the configurations to enable user log on or log off.

#### Parse and apply

Click to parse the XML content and apply the configurations.

The screenshot shows the 'Request XML String' section of the API Explorer. It features a text input field with an asterisk (\*) indicating it is required, and a blue 'Parse and apply' button below it. The entire interface is contained within a light gray border.

**Figure 64: API Explore**

### Sample XML Request Code

For all the requests, XML response will be displayed in a pop-up window.

```
<Request><LiveUserLogin><UserName>sophos</UserName><Password>sophos</Password><IPAddress>10.21.18.15</IPAddress><MacAddress>00:0C:29:2D:D3:AC</MacAddress> </LiveUserLogin></Request>
```

```
<Request><LiveUserLogout><Admin><UserName>admin</UserName><Password>admin</Password></Admin><UserName>sophos</UserName><IPAddress>10.21.18.15</IPAddress></LiveUserLogout></Request>
```

For versions prior to 10.6.1 MR-1

```
<Request><LiveUserLogout><UserName>sophos</UserName><IPAddress>10.21.18.15</IPAddress></LiveUserLogout></Request>
```

Please use the below link to use API:

<https://<Sophos IP>:<port>/webconsole/APIController?reqxml=<Add the XML request here>>

 **Note:** Port you mention in above URL should be same as the port you have configured as **Admin Console HTTPS Port** from **System > Administration > Admin Settings**.

For example:

```
https://<Sophos IP>:4444/webconsole/APIController?
reqxml=<Request><LiveUserLogin><UserName>sophos</UserName><Password>sophos</
Password><IPAddress>10.21.18.15</IPAddress><MacAddress>00:0C:29:2D:D3:AC</
MacAddress></LiveUserLogin></Request>
```



**Note:** When the user logs on using API, the client type of the users will display **API Client** on the **Live Users** page.

## Import Export

You can export and import full or partial device configuration across compatible devices of the same or different models. Device configuration is exported to a text file in human readable XML format. Update it offline, if required.

### Import

#### Import File

To select the complete path of the tar file to be imported, click the file selection button against **Import File**.

#### Import

Click to import the configuration on the device.

Device existing configuration will be preserved. Entities with same name in existing configuration will be updated with the imported entity configuration and new Entities will be added.

For example:

If you have a Network Traffic Quota Policy with name “Daily 10 MB” in both the existing and imported configuration then the existing policy configuration will be updated with the imported configuration. Any new policies in the imported configuration will also get added.

**Figure 65: Import Configuration**

### Export

#### Export full configuration

Select to export all the entities configuration to a text file.

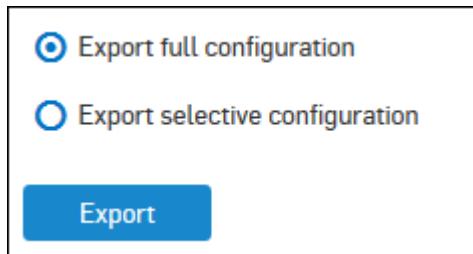
#### Export selective configuration

Select to export only selected entities configuration. Click **Add New Item** to select entities and apply to add the selected entities.

Dependent entities for the selected entity will also be exported if **Include dependent entity** is selected.

### Export

Click to export the configuration from the device.



**Figure 66: Export Configuration**

## Firmware

**This feature is not available in Sophos Firewall Manager (SFM).**

The Firmware page allows you to manage the firmware versions on your device. It also enables you to install hot-fixes and to choose the default configuration language of your device.

The **Firmware** section displays the list of firmware versions that have been downloaded. A maximum of two firmware versions are available simultaneously and one of the versions is active.

### Upload firmware

Click  to upload new firmware. Click **Browse** in the pop-up window. Click **Upload firmware** to upload the firmware image file. The uploaded firmware becomes active after the next reboot.

Click **Upload & Boot** to upload the firmware image file and boot the device. The action upgrades the device to the new version, closes all sessions, restarts the device, and displays the login page. The process may take a few minutes since it involves migrating the entire configuration.

At the time of uploading new firmware, the error “New Firmware could not be uploaded” might occur due to one of the following reasons:

1. Wrong upgrade file - You are trying to upload wrong upgrade file i.e. a previous version firmware.
2. Incorrect firmware image - You are trying to upload incorrect firmware image for your appliance model. All the firmware's are model specific and are not inter-changeable. Hence, firmware of one model is not applicable on another model. For example, an error is displayed, if appliance model XG125 is upgraded with firmware for model XG750.
3. Incompatible firmware - You are trying to upload incompatible firmware.
4. Changes in Appliances Hardware - Your appliance hardware configuration is not the standard hardware configuration. Contact support for assistance.
5. Corrupt firmware - There are chances that the firmware you have downloaded is corrupt.

### Boot firmware image

Click  to upgrade the device to the uploaded firmware image. The action upgrades the device to the new version, closes all sessions, restarts the device and displays the login page.

### Boot with factory default configuration

Click  to reboot the device and to activate the default configuration.

 **Note:** If you boot with factory default configuration, the current configuration will be lost. Take a backup before you click this option.

### Active

The Active icon  against a firmware version indicates that the device currently uses this firmware.

**Latest Available Firmware (*not available in SFM*)****Check For new Firmware**

Click to view the new firmware, if available.

**Firmware Version**

Displays the list of firmware versions available for download.

**Type**

Displays the type of each firmware.

**Available Options:**BetaGA

**Actions**

Click **Download** to download the firmware. Once the download is complete, click **Install** to install the firmware.

			Check for new Firmware
Firmware Version	Type	Actions	
No Records Found			

**Figure 67: Available Latest Firmware**

**SF-OS Hot-fix****Allow auto-install of important Hot-fixes**

Hot-fixes are installed automatically when they are available. Clear the check box if you do not want to apply them automatically.

Click **Apply** to save your selection.

Default: Enabled

<input checked="" type="checkbox"/> Allow auto-install of important Hot-fixes
<b>Apply</b>

**Figure 68: SF-OS Hot-Fix**

**Factory Reset with Default Configuration Language****Default Configuration Language**

Select a default language for configuration. When you choose a different language, the device reboots and goes back to the factory default settings. It removes all customizations.

The Admin Console Language can differ from the Default Configuration Language. Choosing a different Admin Console Language displays menus and labels in the selected language while choosing a different **Default Configuration Language** displays menus, labels as well as default policies and their description in the selected language.

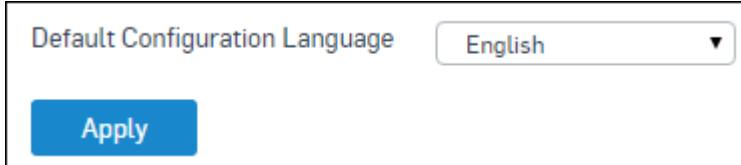
Default: English

**Available Options:**

- English
- Hindi
- Chinese - Traditional

- Chinese - Simplified
- French
- Japanese

 **Note:** Take a backup before you choose a different language since the entire configuration will be lost. The device restores the backup in the language that was operational at the time of taking the backup.



**Figure 69: Factory Reset with Default Configuration Language**

## Pattern Updates

This page displays the status of patterns used by various modules of your device like Sophos AV, IPS and Application Signature, WAF. The page also provides options to update patterns or set an auto-update time interval. By default pattern are updated automatically.

### Updates Status

#### Pattern

Name of the pattern.

#### Current Version

Version of the pattern in use.

#### Available Version

Upgrade version, if available.

#### Last Successful Update

Displays time and date of the last successful update.

#### Status

Displays status of the pattern.

- Ready to Install
- Success
- Downloading
- Failed

#### Update Pattern Now

Click to update the pattern definitions.

Last Checked for updates: 13:14:16, Oct 20 2015 ( Last Successful Check 11:23:26, Sep 29 2015 )				<a href="#">Update Pattern Now</a>
Pattern	Current Version	Available Version	Last Successful Update	
AP Firmware	-	-	-	
ATP	1.0.0027	-	21:23:33, Sep 24 2015	
Authentication Clients	1.0.0010	-	20:41:34, Sep 17 2015	
IPS and Application signatures	3.12.38	-	21:35:54, Aug 12 2015	
RED Firmware	1.0.004	-	11:14:33, Aug 25 2015	
Sophos AV	1.0.0027	-	21:32:16, Sep 24 2015	
SSLVPN Clients	-	-	-	
WAF	1.0.0006	-	-	

**Figure 70: Update Status****Pattern Download/Installation****Auto Update**

To update pattern definitions automatically, click **Auto Update**.

Firmware updates for RED and Access Points are automatically downloaded and a notification is displayed. You have to manually install those updates. Usually, after installation the RED or AP reboots. Connections to REDs or APs will be interrupted during that time and re-established afterwards.

**Interval (Available only if Auto Update is turned ON)**

Set the time limit in which you want to receive updates.

**Available Options:**

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

Auto Update
 ON

Interval
Every 2 hours ▾

Apply

**Figure 71: Pattern download/installations**

# Configure

---

## Network

---

Network section allows you to configure various components for optimal network operation.

In particular, this section covers the following topics:

- [Interfaces](#): Configure and manage the ports/interfaces of the device.
- [Zones](#): Configure custom zone and view the list of default and custom zones.
- [WAN Link Manager](#): Manage device's WAN links.
- [DNS](#): Manage DNS servers to be used by the device, DNS host entries and routing of specific requests.
- [DHCP](#): Manage DHCP servers, relay agent configuration and the list of the IP addresses leased by the device.
- [IPv6 Router Advertisement](#): View the list of configured router advertisements (RA), configure RAs.
- [Cellular WAN](#): Configure parameters of the cellular WAN connection of the device.
- [IP Tunnels](#): Create and manage 6in4, 6to4, 6rd and 4in6 IP tunnels for inter-communication between IPv6 and IPv4 networks.
- [Neighbors \(ARP-NDP\)](#): View and manage device's ARP-NDP neighbors.
- [Dynamic DNS](#): Integrate device with a dynamic DNS. Manage existing configuration.

## Interfaces

**Interfaces** lists all the interfaces of the device along with their configurations.

The device is shipped with a number of physical interfaces, that is, ports and a number of virtual interfaces, depending on the model of the device. The Interface page displays a list of physical interfaces, aliases, virtual interfaces, bridge interfaces, interfaces configured as LAG or as TAP as well as interfaces configured for wireless LAN or for cellular WAN.

**Interfaces** allows you to configure a range of physical and virtual interfaces. If a virtual interface is configured for a physical interface, it is displayed below the physical interface. Virtual interface configuration can be updated or deleted.

 **Note:** Updating the interface details may affect dependent configurations. Refer [Configurations dependent on Interfaces](#) for more details.

The possible configurations are provided below:

- [Alias](#) – Alias allows you to bind multiple IP addresses to a single physical interface.
- [Bridge](#) – A bridge enables you to configure transparent subnet gatewaying.
- [LAG](#) – Link Aggregation Group (LAG) allows multiple network connections to be combined into a single connection. It is also known as trunking, NIC teaming, NIC bonding, or Ether Channel. LAG is mostly used to handle LAN traffic.
- [VLAN](#) – A virtual LAN is a broadcast domain with each VLAN being configured on a switch to individual ports.
- [Wireless Networks](#) – A wireless network links devices through a wireless distribution method, connecting them to the Internet through an access point.

If a wireless network is configured with a “Separate Zone” for [Client Traffic](#) mode under **Protect > Wireless > Wireless Networks**, a `wlnet` interface of the type “Wireless Protection” is automatically created on this page with the configured IP address and zone of the wireless network. In order to use the interface, you need to configure a DHCP server for the interface so that the wireless clients can connect to the device. The interface will automatically be deleted once the wireless network is deleted.

- [Cellular WAN](#) – A cellular WAN is a wide area network (WAN) for data that is typically provided by cellular carriers to transmit a wireless signal over a range of several miles to a mobile device.

- **TAP** – A TAP interface enables you to deploy the device in Discover Mode. In this mode, the device can monitor all the network traffic without making any changes in the existing network schema. Discover Mode can be configured through the command line interface (CLI).
- **RED** - The Remote Ethernet Device (RED) is used to connect remote branch offices to your head office as if the branch office is part of your local network. The RED device connects to the main device using a RED interface and can be configured using this interface. On factory default, all the configured RED interfaces are deleted.

Interface status messages can have the following values:

- **Disabled** - The interface is currently not bound to any zone.
- **Connected** - The interface is connected, configured and is running.
- **Connecting (*Displayed only for PPPoE and cellular WAN (WWAN1) interfaces*)** - Displayed when a new IP address is being leased.
- **Disconnected (*Displayed only for PPPoE and cellular WAN (WWAN1) interfaces*)** - Displayed after the IP address has been released.
- **Disconnecting (*Displayed only for PPPoE and cellular WAN (WWAN1) interfaces*)** - Displayed during the process of IP release.
- **Unplugged** - No physical connection.
- **Not Available (*Applicable for Flexi Ports devices*)** - If the Flexi Ports module has previously been inserted and Flexi Ports have been configured, then after removing the Flexi Ports module from the device, the Flexi Ports will carry the status “Not Available”.

The following list shows the different icons, representing the different interface types:

Icons	Meaning
	Ethernet
	Wireless
	Bridge
	VLAN
	RED10
	RED15
	RED50
	LAG
	WWAN



#### Note: Configurations dependent on Interfaces

- Updating the interface details may affect dependent configurations, including Interface zone binding, DNS, gateway, interface-based hosts, VLAN interfaces, and dynamic DNS.
- Deleting the virtual interface will delete the firewall rule defined for the virtual interface.
- Deleting the interface will also remove all its dependent configurations, including interface zone binding, DHCP server or relay, interface-based firewall rule, ARP (static and proxy), protected servers, protected server-based firewall rules, interface-based hosts and references from host groups as well as unicast and multicast routes.

- Your network connections might get affected for some time after updating/deleting Interfaces. If you face any network issues during this time then please wait for some time and check again.

## Physical Interface Configuration

Use this page to edit physical interface configurations.

1. Go to **Configure > Network > Interfaces**. Identify the physical interface whose settings need to be updated and click the  icon on the right side. Click **Edit Interface** within the box.
2. Enter the details for **General Settings**.

### Physical Interface

Physical interfaces are ports which may be marked in numeric (Port1, Port2, and so on), alphabetic (PortA, PortB, and so on), alphanumeric (PortA2, PortA3, and so on), or in special alphanumeric form (eth0, eth1, and so on), depending on your device.

### Network Zone

Select the zone to which the interface belongs.

Available Options:

- None: Select to unbind the interface.
- LAN
- WAN
- DMZ
- WiFi

Physical Interface	PortA
Network Zone	<input type="button" value="LAN"/>

**Figure 72: General Settings**

3. Enter the **IPv4 configuration** details.

### IP Assignment

Select the IP assignment type.

Available Options:

- **Static** - Click to specify the IP address manually.
- **PPPoE** - Click to enable the interface to receive the IP address from a PPPoE server.
- **DHCP** - Click to enable the interface to receive the IP address dynamically from a DHCP server.

### IPv4/Netmask

Enter the IPv4 address of the interface. Select the network subnet mask.

### Preferred IP (*available only if selected IP Assignment is PPPoE*)

Many Internet service providers assign a static IP address to PPPoE connections. The device allows you to bind the static IP address to the PPPoE connection.



**Note:** An IP Address other than the preferred IP Address may be assigned to the PPPoE connection, depending on the PPPoE Server configuration.

4. Enter the IPv4 gateway details.

### Gateway Detail (*available only for WAN zone*)

- **Static IP Assignment** - Enter the Gateway Name and the IPv4 address through which traffic is to be routed.
- **PPPoE IP Assignment** - Enter the Gateway Name through which traffic is to be routed.
- **DHCP IP Assignment** - Enter the Gateway Name through which traffic is to be routed.

The screenshot shows the 'IPv4 Configuration' section. At the top, there is a checked checkbox labeled 'IPv4 Configuration'. Below it, there are three radio button options: 'Static' (selected), 'PPPoE', and 'DHCP'. Under 'IP Assignment', there are two input fields: 'IPv4/Netmask \*' containing '10.198.15.35' and a dropdown menu showing '/23 (255.255.254.0)'. Below these are three empty input fields for 'Gateway Detail': 'Gateway Name' and 'Gateway IP', and an empty input field for 'Gateway IP'.

**Figure 73: IPv4 Configuration**

- Enter the details for PPPoE IP Assignment.

#### Username

Enter the PPPoE account username.

#### Password

Enter the PPPoE account password.

#### Access Concentrator/Service Name

Enter the access concentrator and service name.

The device initiates only those sessions with the access concentrator that can provide the specified service.

#### LCP Echo Interval

Enter the time interval at the end of which the system sends an echo request to check whether the link is alive. Once an attempt is made, the device waits for the defined time interval before the next attempt is made.

Default: 20 seconds

#### LCP Failure

Enter the number of attempts (echo requests) to be made. Once the specified number of attempts are made without receiving a response from the client, the device disconnects the PPPoE connection.

Default: 3

#### Schedule Time For Reconnect

The IP address assigned to a PPPoE connection, whether dynamic or static (preferred), can have a predefined validity period. Once the validity expires, the PPPoE connection is terminated and is reconnected.

To prevent reconnection during working hours, enable the PPPoE reconnect schedule. You may choose to schedule the PPPoE reconnection on daily or weekly basis at the configured time (HH:MM).

Default: Disabled

Default schedule when enabled: All days of the week



**Note:** Even when a Preferred IP address has been configured, if Schedule Time For Reconnect is enabled and configured, on reconnection, an IP address other than the preferred IP address may be assigned to the PPPoE connection.

The screenshot shows the PPPoE configuration interface. It includes fields for 'Username \*' (text input), 'Password \*' (text input), 'Confirm Password' (text input), 'Access Concentrator/Service Name' (text input), and two dropdowns separated by a slash. Below these are several configuration options with checkboxes:

- LCP Echo Interval: Send LCP echo request every  seconds (5-180, Default:20)
- LCP Failure: Wait for LCP echo reply for  attempts (Default:3)
- Schedule Time for Reconnect: A dropdown menu showing 'All days of the week' followed by time fields (00:00:00 MM).

**Figure 74: PPPoE Configuration****6. Enter the IPv6 configuration details.****IP Assignment**

Select the IP assignment type.

Available Options:

- Static
- DHCP

**Mode (*only for DHCP mode*)**

Select the DHCP mode.

Select the relevant option to configure the IPv6 addresses through stateful (DHCPv6) or Stateless address assignment methods depending on the Managed (M) Address Configuration and Other (O) configuration flags advertised in the Router Advertisement (RA) message.

Available Options:

**Auto** - If selected, the IPv6 address will be configured based on the router advertisement packet through Stateless Address Auto-Configuration (SLAAC) or through DHCPv6 depending on the Managed (M) Address Configuration and Other (O) Configuration flags advertised in the Router Advertisement (RA) message. **Manual** - Select the relevant option to configure the IPv6 address either through SLAAC or through DHCPv6.

- **DHCP Only** - In this manual mode, the client will configure IPv6 Address and other configuration parameters using DHCPv6 Server. Gateway details should be manually specified.
- **Stateless** - In this manual mode, client will configure IPv6 Address based on advertised RA message through SLAAC.
  - **Accept Other Configuration from DHCP:** Select to configure other parameters using DHCPv6 Server. By default, it is enabled.

**DHCP Rapid Commit**

If enabled, the interface will be configured using a 2-message exchange (Solicit and Reply) rather than the 4-message exchange (Solicit, Advertise, Request, and Reply). It allows for quicker client configuration.

 **Note:** Rapid commit should also be enabled on the DHCPv6 server.

**IPv6 / Prefix (*Only for static IP assignment*)**

Enter the IPv6 address and the prefix.

**Gateway Detail (*Only for “WAN” zone*)**

**For Static IP assignment:** Enter the gateway name and IPv6 address through which the traffic is to be routed. **For DHCP IP assignment:** Enter the gateway name, if **Stateless** manual mode is selected. For **DHCP only** manual mode, specify the gateway name and IPv6 address.

The screenshot shows the configuration interface for IPv6. Under 'IP Assignment', 'DHCP' is selected. Under 'Mode', 'Auto' is selected. There are three radio buttons for 'DHCP Only', 'Stateless', and 'Accept other configuration from DHCP', with 'Accept other configuration from DHCP' checked. Under 'DHCP Rapid Commit', there is an unchecked checkbox. The 'IPv6/Prefix' field contains '64'. Under 'Gateway Detail', there are two empty text input fields for 'Gateway Name' and 'Gateway IP'.

**Figure 75: IPv6 Configuration - DHCP**

## 7. Enter details for the Advanced Settings.

### Interface Speed

Select interface speed for synchronization. Interface speed can also be configured through CLI using `set network interface-speed` command.

Speed mismatch between the device and third-party routers and switches can result in errors or collisions on the interface, disconnection, traffic latency, or slow performance.

**Depending on the model deployed, the following options are available:**

Auto Negotiation 10 Mbps - Half Duplex 10 Mbps - Full Duplex 100 Mbps - Half Duplex 100 Mbps - Full Duplex 1000 Mbps - Full Duplex

Default - Auto Negotiation

### MTU

Enter the MTU (Maximum Transmission Unit) value.

MTU is the largest physical packet size, in bytes, that a network can transmit. This parameter becomes an issue when networks are interconnected and the networks have different MTU sizes. Any packets larger than the MTU value are divided (fragmented) into smaller packets before being sent.

Default - 1500

Acceptable Range (*For IPv4 Configuration*): 576 to 1500

Acceptable Range (*For IPv6 Configuration*): 1280 to 1500

### Override MSS

Select to override the default MSS.

MSS defines the amount of data that can be transmitted in a single TCP packet.

Default: 1460

Acceptable Range: 536 to 1460

### Use Default MAC Address

Click to use the default MAC address for the interface.

By default, the first port that is included as member port becomes the default MAC address.

#### Override Default MAC Address

Click to override the default MAC address for the interface and enter the new MAC address.

On factory reset, it is set to the default MAC Address.

Interface Speed	Auto Negotiation
MTU	1500 (1280-1500)
<input type="checkbox"/> Override MSS	1460 (536 - 1460)
<input checked="" type="radio"/> Use Default MAC Address	00.00.48.26.6C.7F
<input type="radio"/> Override Default MAC Address	

**Figure 76: Advanced settings**

8. Click Save.

### Advanced Settings for Bridge Interface

1. Go to **Configure > Network > Interfaces**. Identify the bridge interface whose advanced settings need to be updated and click the  icon on the right-hand side. Click **Edit Interface** within the box.
2. Enter the details for Advanced Settings.

#### Physical Interface

Displays the physical bridge member interface.

#### Network Zone

Displays the zone to which the physical interface belongs.

#### Interface Speed

Select the interface speed for synchronization. Interface speed can also be configured through CLI using the `set network interface-speed` command.

Speed mismatch between the device and third-party routers and switches can result in errors or collisions on the interface, disconnection, traffic latency, or slow performance.

Depending on the device, the following options are available:

- Auto Negotiation
- 10 Mbps - Half Duplex
- 10 Mbps - Full Duplex
- 100 Mbps - Half Duplex
- 100 Mbps - Full Duplex
- 1000 Mbps - Full Duplex

Default: Auto Negotiation.

#### MTU

Enter the MTU (Maximum Transmission Unit) value. MTU is the largest physical packet size (in bytes) that a network can transmit.

Default: 1500

#### Override MSS

Select the checkbox to override the default MSS (Maximum Segment Size). MSS defines the amount of data that can be transmitted in a single TCP packet.

Default: 1460

#### Use Default MAC Address

Click to use the default MAC address of the interface. The MAC address of the first port to be added as member port becomes the default MAC address.

#### Override Default MAC Address

Click to override the default MAC address of the interface and enter the new MAC address. On factory reset, it will be set to the default MAC address.

Physical Interface	PortE
Network Zone	DMZ
Interface Speed	<input type="button" value="Auto Negotiation"/>
<input checked="" type="radio"/> Use Default MAC Address	<input type="text" value="00:0D:48:26:6C:83"/>
<input type="radio"/> Override Default MAC Address	<input type="text"/>

**Figure 77: Advanced Settings - Bridge Interface**

3. Click Save.

#### Add Bridge

This feature is not supported when the device is deployed on Microsoft Hyper-V hypervisors.

1. Go to **Configure > Network > Interfaces**, click **Add Interface** on the right side and click **Add Bridge** from the drop-down list.
2. Enter the details for **General Settings**.

##### Name

Enter a name to identify the bridge.

##### Description

Enter a description for the bridge.

##### Enable routing on this bridge pair

Select the checkbox to enable routing on this bridge.

Name *	<input type="text" value="Enter Name"/>
Description	<input type="text" value="Enter Description"/>
<input type="checkbox"/> Enable routing on this bridge pair	

**Figure 78: General Settings**

3. Enter the details of **Member Interfaces**.

##### Interface

Select the interfaces of the bridge. For example, Port A, Port B.

##### Zone

For each interface, select the zone to which the interface belongs.

Interface	Zone	<b>+</b>
Select Interface	Select Zone	
Select Interface	Select Zone	

**Figure 79: Bridge Member Interfaces**

- Enter IPv4 configuration and gateway details.

**IPv4 / Netmask**

Enter the IPv4 address and select the network subnet mask.

**Gateway Name**

Enter a name to identify the gateway.

**Gateway IP**

Enter the IPv4 address for the gateway.

IPv4/Netmask *	<input type="text"/>	/24 (255 255 255 0)
Gateway Detail		
Gateway Name	<input type="text"/>	
Gateway IP	<input type="text"/>	

**Figure 80: IPv4 Configuration and Gateway Details**

- Enter the **IPv6 configuration** details.

**IPv6 / Prefix**

Enter the IPv6 address and the prefix.

**Gateway Name**

Enter a name to identify the gateway.

**IP Address**

Enter the IPv6 address for the gateway.

IPv6/Prefix *	<input type="text"/> / 64	
Gateway Detail		
Gateway Name	<input type="text"/>	
Gateway IP	<input type="text"/>	

**Figure 81: IPv6 Configuration**

- Enter the details for **Advanced Settings**.

**MTU**

Enter the MTU (Maximum Transmission Unit) value.

MTU is the largest physical packet size (in bytes) that a network can transmit. Problem arises when networks with differing MTU sizes are interconnected. In such a scenario, packets larger than the specified MTU value are divided (fragmented) into smaller packets before they are sent.

Default: 1500

Acceptable Range (*For IPv4 Configuration*): 576 to 1500

Acceptable Range (*For IPv6 Configuration*): 1280 to 1500

### Override MSS

Select the checkbox to override the default MSS (Maximum Segment Size).

MSS defines the amount of data that can be transmitted in a single TCP packet.

Default: 1460

Acceptable Range: 536 to 1460

The screenshot shows a configuration interface for advanced settings. It includes fields for MTU (set to 1500) and Override MSS (checkbox checked, set to 1460). The acceptable range for MTU is 1280-1500, and for Override MSS it is 536 - 1460.

MTU	1500	(1280-1500)
<input checked="" type="checkbox"/> Override MSS	1460	(536 - 1460)

**Figure 82: Advanced Settings**

### Note:

- A single WAN interface is supported in a bridge.
- A single interface cannot be part of multiple bridges.

7. Click **Save**.

## Add Alias

Use this page to bind multiple IP addresses to a single interface.

1. Go to **Configure > Network > Interfaces**, click **Add Interface** on the right side and click **Add Alias** from the drop-down list.
2. Enter the interface details.

### Physical Interface

Select the interface to which an Alias must be bound.

### IP Family

Select the IP family for the Alias.

### Available Options:

IPv4 (*Only for physical interfaces with IPv4 configuration*)

IPv6 (*Only for physical interfaces with IPv6 configuration*)

### IPv4/Netmask (*Available only if IP Family selected is IPv4*)

Enter the IPv4 address and select the network subnet mask.

### IPv6/Prefix (*Available only if IP Family selected is IPv6*)

Enter the IPv6 address and the prefix.

Default: 64

The screenshot shows the 'Add Alias' configuration page. It includes fields for Physical Interface (DocTeam), IP Family (IPv4 selected), and IPv4 / Netmask (/24 (255 255 255 0)).

Physical Interface *	DocTeam
IP Family *	<input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6
IPv4 / Netmask *	/24 (255 255 255 0)

**Figure 83: Add Alias**

### 3. Click **Save**.

#### Related tasks

[Add NAT Policy](#) on page 60

To enable internal hosts to access the Internet through a public IP address, create a Network Address Translation (NAT) policy. The policy specifies the public IP addresses through which NATing can take place. The NAT policy must then be applied to a **Firewall Rule** (**Protect > Firewall**).

## Configure Cellular WAN Settings

Enable **Cellular WAN** from **Configure > Network > Cellular WAN**.

1. Go to **Configure > Network > Interfaces**. Identify the cellular WAN (WWAN1) interface whose settings need to be updated and click the  icon on the right side. Click **Edit Interface** within the box.
2. Enter the details for General Settings.

#### Interface Name

Enter a name for the interface.

#### IP Assignment

Select the IP assignment method from the available options:

**Available Options:** Dial-up (PPP) Network Adapter (DHCP)

#### Show Recommended Configuration

Click to view the modem details and the recommended configuration. The recommended configuration is displayed in two sections:

##### Information Section:

- Modem Name
- Vendor ID
- Product ID
- SIM PIN Enabled – Yes/No

##### Configuration Section:

Available IP Assignment Methods:

Possible Values

- Dial-up (PPP)
- Network Adapter (DHCP)
- Dial-up (PPP) & Network Adapter (DHCP)

#### Modem Port:

Possible Values

- Not Available
- Serial n (n= 0, 1, ...9)

#### Secondary Modem Ports:

Possible Values

- Not Available
- Serial n (n = 0, 1, ...9)



**Note:** This parameter displays the next available modem port. This port must be used as the **Modem Port**, if the recommended modem port fails.

#### APN (Access Point Name):

Possible Values

- Not Available
- <name>

**DHCP Connect Command:**

Possible Values

- Not Required
- Required but not available
- <AT command>

**DHCP Disconnect Command:**

Possible Values

- Not Required
- Required but not available
- <AT command >

Click **Load Recommended Configuration** to load the recommended configuration onto the page. This action removes previous configurations, if any, and replaces them with the recommended configuration.



**Note:** When you click **Load Recommended Configuration**, values of the secondary modem ports are not loaded.

**Connect**

Select the mode to establish a cellular WAN connection.

**Available Options:**AutoManual

**Reconnect Tries**

Select the number of attempts to be made when reconnecting to an access point.

**Available Options:**Always123Default: **Always**

**Modem Port (*Available only if IP Assignment selected is Dial-up (PPP)*)**

Enter the serial interface on which the modem will establish a connection.

**Available Options:**Serial 0 to 9

**Phone Number (*Available only if IP Assignment selected is Dial-up (PPP)*)**

Enter the phone number to be used in order to establish the connection or select one from the drop-down list.

**Username**

Enter a username for the connection.

**Password**

Enter a password.

**SIM Card PIN Code**

Enter the PIN code in order to unlock the PIN-enabled SIM card.

Many operators lock their SIM card to prevent the use of another operator's SIM card. Such modems can be unlocked using the PIN code in order to establish a connection.

**APN**

Enter the Access Point Name (APN).

The APN is a configurable network identifier based on which the device identifies the Packet Data Network (PDN) or the GSM carrier with which the user wants to communicate.

**DHCP Connect Command (*Available only if IP Assignment selected is Network Adapter (DHCP)*)**

Enter a DHCP command to connect to the cellular WAN.

**DHCP Disconnect Command (*Available only if IP Assignment selected is Network Adapter (DHCP)*)**

Enter a DHCP command to disconnect from the cellular WAN.

### Initialization String

Enter an initialization string for the specific wireless modem. In case of multiple strings, the strings must be entered in the order of their priority.

Interface Name	WWAN1
IP Assignment *	<input checked="" type="radio"/> Dial-up (PPP) <input type="radio"/> Network Adapter (DHCP)
Connect *	<input checked="" type="radio"/> Auto <input type="radio"/> Manual
Reconnect Tries *	Always
Modem Port *	Serial 0
Phone Number *	Select/Add
Username	
Password	
SIM Card PIN Code	
APN	
Initialization String	<input type="text"/> <span style="margin-left: 10px;">Initialization String</span> <span style="margin-left: 10px;">+</span> <span style="margin-left: 10px;">-</span>

**Figure 84: General Settings - Dial-up**

3. Enter the details for Gateway Settings.

#### Gateway Name

Enter a name to identify the gateway.

#### Gateway IP

Enter the IP address of the gateway.

Gateway Name *	WWAN1_GW
Gateway IP	128.0.0.1

**Figure 85: Gateway Settings**

4. Enter the details for Advanced Settings.

#### MTU

Enter the MTU (Maximum Transmission Unit) value.

MTU is the largest physical packet size (in bytes) that a network can transmit. Problem arises when networks with differing MTU sizes are interconnected. In such a scenario, packets larger than the specified MTU value are divided (fragmented) into smaller packets before they are sent.

Default: 1500

Acceptable Range: 576 to 1500

#### MSS

Enter the MSS (Maximum Segment Size).

MSS is the amount of data that can be transmitted in a single TCP packet.

Default: 1460

Acceptable Range: 536 to 146

#### **MAC Address (*Available only if IP Assignment selected is Network Adapter (DHCP)*)**

Select the method of providing a MAC address to the modem:

**Available Options:** Use Default MAC AddressOverride Default MAC Address (If you select this option, provide the MAC address.)

The screenshot shows a configuration interface for 'Other Settings'. It includes two input fields: 'MTU \*' with the value '1500' and 'MSS \*' with the value '1460'. Both fields have a blue asterisk indicating they are required.

**Figure 86: Other Settings**

5. Click Save.

### **Virtual LAN (VLAN)**

VLANs are virtual LANs in which work devices on one or more LANs are logically segregated into independent broadcast domains. The logical segregation allows devices from multiple LANs across different floors or geographical regions to communicate as if they are physically connected. At the same time, a single LAN can be separated into multiple VLANs based on roles, work groups, services, or any other logical parameter.

Although routers are generally used to create broadcast domains in LANs, switches create the VLAN broadcast domains. You can assign each VLAN to one or more ports on a single switch. In case of distributed VLANs, you can assign them across multiple switches. Communication within a VLAN happens through the switch, while communication across different VLANs requires a layer 3 device – a router, a layer 3 switch, or a firewall.

You can implement VLAN technology between a Sophos Firewall (SF) device and 802.1Q-compliant switches and routers. Tag-based LAN multiplexing technology simulates multiple LANs within a single physical LAN and traffic from each broadcast domain is given a different VLAN tag. VLAN IDs/tags are 4-byte frame extensions that contain a VLAN identifier and information specific to your configuration.

SF recognizes VLAN IDs, allowing you to apply firewall rules specific to each VLAN, including authentication and other relevant policies of your network. You can also apply firewall rules to secure the network between broadcast domains.

#### **Advantages**

- Increase in the number of ports
- Logical segmentation of network regardless of physical location
- Granular firewall rules specific to workgroups
- Improved network throughput due to the creation of smaller broadcast domains

#### **Add VLAN Interface**

1. Go to **Configure > Network > Interfaces**, click **Add Interface** on the right side and select **Add VLAN** from the drop-down list.
2. Enter the VLAN details.

#### **Physical Interface**

Select a parent interface for the virtual sub-interface. The virtual sub-interface becomes a member of the selected physical interface.

#### **Zone**

Select a zone to assign to the virtual sub-interface. The virtual sub-interface becomes a member of the selected zone which can be LAN, DMZ, WAN, WiFi or a custom zone.

## VLAN ID

Enter the VLAN ID. The interface VLAN ID can be any number between 2 and 4094. The VLAN ID of each virtual sub-interface must match the VLAN ID of the packet. If the IDs do not match, the virtual sub-interface will not receive the VLAN-tagged traffic.



**Note:** When added to the same physical interface, more than one virtual sub-interface cannot carry the same VLAN ID. However, virtual sub-interfaces carrying the same VLAN ID can be added to different physical interfaces.

Physical Interface *	<input type="text" value="PortA"/>
Zone *	<input type="text" value="LAN"/>
VLAN ID *	<input type="text"/>

**Figure 87: VLAN Details**

3. Enter the IPv4 configuration details (**Only for physical interfaces with IPv4 configuration**).

### IP Assignment

Select the IP assignment type.

#### Available Options:

- Static
- PPPoE
- DHCP

### IPv4/Netmask

Enter the IPv4 address for the interface and select the network subnet mask.

### Preferred IP (*available only if IP Assignment selected is PPPoE*)

Many Internet service providers assign a static IP address to PPPoE connections. The device allows you to bind the static IP address to the PPPoE connection.

Enter the preferred IP address for the PPPoE connection.

### Gateway Detail (*For “WAN” zone*)

- **Static IP Assignment:** Specify the Gateway Name and the IPv4 address through which the traffic is to be routed.
- **PPPoE IP Assignment:** Specify the Gateway Name through which the traffic is to be routed.
- **DHCP IP Assignment:** Specify the Gateway Name through which the traffic is to be routed.

IP Assignment	<input checked="" type="radio"/> Static <input type="radio"/> PPPoE <input type="radio"/> DHCP
IPv4/Netmask *	<input type="text" value="/24 (255.255.255.0)"/>
Gateway Detail	<input type="text"/>
Gateway Name	<input type="text"/>
Gateway IP	<input type="text"/>

**Figure 88: IPv4 Configuration**

4. Enter the details for PPPoE IP Assignment.

### Username

Enter the PPPoE account username.

**Password**

Enter the PPPoE account password.

**Access Concentrator/Service Name**

Enter the access concentrator and service name.

The device initiates only those sessions with the access concentrator that can provide the specified service.

**LCP Echo Interval**

Enter the length of time that the system must wait before it sends an echo request to check whether the link is alive. Once an attempt is made, the device waits for the defined time interval before the next attempt is made.

Default: 20 seconds

**LCP Failure**

Enter the number of attempts (echo requests) to be made. Once the specified number of attempts are made without receiving a response from the client, the device disconnects the PPPoE connection.

Default: 3

**Schedule Time For Reconnect**

The IP address assigned to a PPPoE connection, whether dynamic or static (preferred), can have a predefined validity period. Once the validity expires, the PPPoE connection is terminated and is reconnected.

To prevent reconnection during working hours, enable the PPPoE reconnect schedule. You may choose to schedule the PPPoE reconnection on daily or weekly basis at the configured time (HH:MM).

Default: Disabled

Default schedule when enabled: All days of week



**Note:** Even when a **Preferred IP** address has been configured, if **Schedule Time For Reconnect** is enabled and configured, on reconnection, an IP address other than the preferred IP address may be assigned to the PPPoE connection.

Username *	<input type="text"/>		
Password *	<input type="password"/> <input style="margin-top: 5px;" type="password"/>		
Service Name	<input type="text"/> <input type="text"/>		
<input type="checkbox"/> LCP Echo Interval	Send LCP echo request every <input type="text" value="20"/> seconds (5-180, Default:20)		
<input type="checkbox"/> LCP Failure	Wait for LCP echo reply for <input type="text" value="3"/> attempts (Default:3)		
<input type="checkbox"/> Schedule Time for Reconnect	All days of the week: <input type="button" value="00"/> <input type="button" value="00"/> HH <input type="button" value="00"/> MM		

**Figure 89: PPPoE Configuration**

- Enter the IPv6 configuration details (*Only for physical interfaces with IPv6 configuration*)

**IP Assignment**

Select the IP assignment type.

**Available Options:**

- **Static**
- **DHCP**

#### **Mode (*available only if IP Assignment selected is DHCP*)**

Select DHCP mode.

Administrator can select to configure IPv6 address through Stateful (DHCPv6) or StateLess address assignment methods depending on the Managed (M) Address Configuration and Other (O) Configuration flags advertised in the Router Advertisement (RA) message .

Available Options:

**Auto:**If selected, IPv6 address will be configured based on the Router Advertisement packet through Stateless Address Auto-Configuration (SLAAC) or DHCPv6 depending on the Managed (M) Address Configuration and Other (O) Configuration flags advertised in the Router Advertisement (RA) message. **Manual:**Administrator can select to configure IPv6 address either through SLAAC or DHCPv6.

- **DHCP Only:**In this manual mode, client will configure IPv6 Address and other configuration parameters using DHCPv6 Server. Gateway details should be manually specified.
- **Stateless:**In this manual mode, client will configure IPv6 Address based on advertised RA message through SLAAC.
  - **Accept Other Configuration from DHCP:** Select to configure other parameters using DHCPv6 Server. By default, it is enabled.

#### **DHCP Rapid Commit**

If enabled, the interface will be configured using a 2-message exchange (Solicit and Reply) rather than the 4-message exchange (Solicit, Advertise, Request, and Reply). It enables quicker client configuration.



**Note:** Rapid commit should also be enabled on the DHCPv6 server.

#### **IPv6 / Prefix (*Only for static IP assignment*)**

Enter the IPv6 address and the prefix.

#### **Gateway Detail (*Only for “WAN” zone*)**

- **For “Static” IP assignment:**Specify the gateway name and IPv6 address through which the traffic is to be routed.
- **For “DHCP” IP assignment:**Specify the gateway name, if **Stateless** manual mode is selected. For **DHCP only** manual mode, specify the gateway name and the IPv6 address.

The screenshot shows the 'IPv6 Configuration' section of the Sophos XG Firewall's Network > Interfaces configuration. The 'IP Assignment' field is set to 'DHCP' (radio button selected). The 'Mode' field is set to 'Auto' (radio button selected). Under 'DHCP', there are three options: 'DHCP Only' (radio button), 'Stateless' (radio button), and 'Accept other configuration from DHCP' (checkbox checked). The 'IPv6/Prefix' field contains '2001:db8::/64'. Below it are fields for 'Gateway Detail', 'Gateway Name', and 'Gateway IP'.

**Figure 90: IPv6 Configuration**

6. Click Save.

## Link Aggregation Group

**LAG is not supported in Sophos virtual security devices.**

Link Aggregation Group (LAG) combines multiple physical links into a single logical link, connecting the SF device to another network device (switch). Also known as trunking, NIC teaming, NIC bonding or Ether Channel, LAG provides redundancy – when one interface fails, the remaining interfaces continue to carry the LAN traffic, ensuring continuity within the network.

### LACP

Link Aggregation Control Protocol (LACP) is part of the IEEE specification 802.3ad and provides additional LAG functionality. You can assign load sharing across links based on the algorithm applied in the xmit hash policy. Link aggregation increases the bandwidth available without the need to deploy additional hardware.

The SF device supports the following LAG modes:

- Active Backup: This mode provides automatic link failover. One link (member of the LAG) remains active while the other remains in standby mode. When the active link fails, the standby link becomes active.
- LACP (802.3ad): This mode provides load balancing and automatic failover. In this mode, all the links are used to forward traffic.

### Prerequisites for LACP (802.3ad) mode

- For LACP to be functional, it must be enabled at both ends of the link.
- All the member interfaces (ports) in the LAG must be of the same type and have the same interface speed.
- All the links must be full-duplex.

### Limitations

- Only unbound static physical interfaces can be members of the LAG.
- PPPoE, 3G, 4G, Cellular WAN, WLAN and Transport mode are not supported in LAG.
- A maximum of 4 ports can be configured on a single LAG interface.

### Add Link Aggregation Group (LAG)

1. Go to **Configure > Network > Interfaces**, click **Add Interface** on the right-hand side and click **Add LAG** from the drop-down list.

LAG interface properties can be configured or edited from the command line, but a LAG interface cannot be added from CLI.

- Enter the details for **Global Settings**.

#### Interface Name

Enter a name for the LAG interface.

#### Member Interface

Click **Add New Item**. The drop-down list displays all unbound ports.

Select the checkbox to select the port(s).



#### Note:

- At least 2 member ports are required to create a LAG interface.
- A maximum of 4 ports can be configured on a single LAG interface.
- Interfaces that have been configured for PPPoE, Cellular WAN or WLAN cannot participate in LAG.

#### Mode

Select the mode of LAG.

#### Available Options:

**Active-Backup:** Select the Active-Backup mode to provide failover. **802.3ad (LACP):** Select the 802.3ad (LACP) mode to load balance the traffic in addition to providing failover.

#### Network Zone

Select the network zone for the interface.

#### Available Options:

LAN WAN DMZ WiFi

Interface Name *	<input type="text"/>
Member Interface *	<input type="button" value="Add New Item"/>
Mode *	<input type="button" value="802.3ad (LACP)"/>
Network Zone *	<input type="button" value="LAN"/>

**Figure 91: Global Settings**

- Enter the IPv4 configuration details.

#### IP Assignment

Select the type of IP assignment.

#### Available Options:

Static DHCP

#### IPv4/Netmask

Enter the IPv4 address for the interface and select the network subnet mask.

- Enter the IPv4 gateway details (*Available only if Network Zone selected is WAN*)

#### Gateway Name

Enter the gateway name.

#### IPv4 Address

Enter the gateway IPv4 address.

IP Assignment       Static  DHCP

IPv4/Netmask \*       /24 (255.255.255.0)

Gateway Detail

Gateway Name

Gateway IP \*

**Figure 92: IPv4 Configuration - Static**

- Enter the **IPv6 configuration** details.

**IPv6/Prefix**

Enter the IPv6 address and the prefix.

- Enter the IPv6 gateway details (*Available only if Network Zone selected is WAN*).

**Gateway Name**

Enter the gateway name.

**IPv6 Address**

Enter the gateway IPv6 address.

IPv6/Prefix \*       / 64

Gateway Detail

Gateway Name

Gateway IP

**Figure 93: IPv6 Configuration**

- Enter the details for **Advanced Settings**.

**Interface Speed**

Select the interface speed for synchronization. Interface speed can also be configured through CLI using the `set network interface-speed` command.

Speed mismatch between the device and third-party routers and switches can result in errors or collisions on the interface, disconnection, traffic latency, or slow performance.

Default: Auto Negotiation

**MTU**

Enter the MTU (Maximum Transmission Unit) value.

MTU is the largest physical packet size (in bytes) that a network can transmit. Problem arises when networks with differing MTU sizes are interconnected. In such a scenario, packets larger than the specified MTU value are divided (fragmented) into smaller packets before they are sent.

Default: 1500

Acceptable Range (*For IPv4 Configuration*): 576 to 1500

Acceptable Range (*For IPv6 Configuration*): 1280 to 1500

**Override MSS**

Select the checkbox to override the default MSS (Maximum Segment Size).

MSS defines the amount of data that can be transmitted in a single TCP packet.

Default: 1460

Acceptable Range: 536 to 1460

#### Xmit Hash Policy (*Available only if Mode selected is LACP (802.3ad)*)

Select the Xmit hash policy to be applied to the member interfaces from the available options in the drop-down list:

##### Available Options:

**Layer2:** Select to generate the hash value using MAC Addresses. **Layer2+3:** Select to generate the hash value using a combination of Layer 2 (MAC Address) and Layer 3 (IP Address) protocol information. **Layer3+4:** Select to generate the hash value using Transport layer protocol information.

#### Primary Interface (*Available only if Mode selected is Active-Backup*)

Select an interface to be the primary interface. This interface remains active as long as it is available.

Default: Auto

The interfaces included in the member interface list are listed here. If you set the **Primary Interface** to **Auto**, the device selects any interface from the member interface list as the primary interface.

#### Use Default MAC Address

Click to use the default MAC address of the interface.

#### Override Default MAC Address

Click to override the default MAC address of the interface and enter the new MAC address.

On factory reset, it will be set to the default MAC address.

Interface Speed	Auto Negotiation
MTU	1500 (1280-1500)
<input checked="" type="checkbox"/> Override MSS	1460 (536 - 1460)
Xmit hash policy	Layer2
<input type="radio"/> Use Default MAC Address	
<input type="radio"/> Override Default MAC Address	

**Figure 94: Advanced Settings**

8. Click Save.

#### Add RED

This page allows you to configure a Remote Ethernet Device (RED) at a remote office.

1. Ensure that RED is activated. This can be done from **Configure > System Services > RED**.
2. Go to **Configure > Network**, click **Add Interface** on the upper right and select **Add RED** from the drop-down list.
3. Enter the **RED Settings** details.

#### Branch Name

Enter the name for the remote location in which the RED is to be set up.

#### Type

Select the RED device to be connected from the drop-down list.

- RED 10
- RED 15
- RED 15w
- RED 50
- Firewall RED Server
- Firewall RED Client
- Firewall RED Server Legacy
- Firewall RED Client Legacy



**Note:** RED device **Firewall RED Server Legacy** and **Firewall RED Client Legacy** are able to connect Sophos XG Firewall with Sophos UTM via RED Site2Site. For more information, see [RED Site-to-Site between Sophos XG Firewall and Sophos UTM](#) on page 126.

#### **RED ID (not available for Type Firewall RED Server, Firewall RED Server Legacy, Firewall RED Client and Firewall RED Client Legacy)**

Enter the **RED ID**.

The RED ID is a 15-character string printed on the sticker which is stuck to the bottom of the RED device as well as on the front of the carton.

#### **Tunnel ID (not available if Type is Firewall RED Client and Firewall RED Client Legacy)**

Select the Tunnel ID from the drop-down list.

By default, **Automatic** is selected. Tunnels are numbered consecutively. Select a unique tunnel ID and make sure that it is the same for both the devices - **RED** and **Sophos XG Firewall**.



**Note:** If the type is **Firewall RED Server Legacy** or **Firewall RED Client Legacy** make sure that the tunnel ID is available on the appliance that should be connected.

#### **Unlock Code**

Enter the unlock code. (Do not fill this field if this RED is being deployed for the first time.)

The unlock code is an 8-character string that is generated when a RED is added to a Sophos XG Firewall. If this RED has been deployed before, you must enter the unlock code here. The unlock code is generated during the deployment of a RED device, and is emailed instantly to the address you provided by activating RED. This is a security feature, which ensures that a RED device cannot simply be removed and installed elsewhere.

For manual deployment through USB stick and for automatic deployment through Provisioning Service (see [Device Deployment](#) below), two separate unlock codes are generated. If you switch a RED device from one deployment method to the other, make sure that you use the corresponding unlock code: For manual deployment, provide the unlock code of the previous manual deployment; for automatic deployment, provide the unlock code of the previous automatic deployment.

#### **Firewall IP/Hostname (not available for Type Firewall RED Server and Firewall RED Server Legacy)**

Enter the hostname of the Sophos XG Firewall.

The hostname must be a publicly resolvable DNS name or IP address for the Sophos XG Firewall. The RED will use this name or the IP address to connect back to the Sophos XG Firewall.

#### **2nd Firewall IP/Hostname (not available if client Type is RED 10)**

Specify the hostname of the second Sophos XG Firewall.

#### **Use 2nd IP/Hostname for (not available if client Type is RED 10)**

Select from the following options:

- **Failover:** Ensures that the secondary Sophos XG Firewall takes over when the primary Sophos XG Firewall fails. The secondary host takes over automatically without loss of connection.
- **Load Balancing:** Distributes traffic equally between, the primary and the secondary Sophos XG Firewall.

### Provisioning File (*available only if Type is Firewall RED Client or Firewall RED Client Legacy*)

To provide the configuration data to the remote client device. Upload the provisioning file using the **Browse** button and transfer the file to the remote device.

#### Description

Enter a description for the RED interface.

#### Device deployment

Select the deployment method:

- **Automatically via Provisioning Service**
- **Manually via USB Stick**



**Note:** If you select manual deployment, it is extremely important to retain the unlock code, which is sent by email. If you lose the unlock code, you can never connect the RED device again to another Sophos XG Firewall and you have to contact the Sophos Support.

By default, Sophos XG Firewall provides the RED's configuration data automatically via Sophos' RED Provisioning Service. In this case, the RED device receives its configuration via Internet. If the RED does not have an Internet connection, you can provide the configuration manually, via USB stick. If you deploy a RED device manually, you have to ensure that the Sophos XG Firewall is acting as NTP server. Activate the NTP on the Sophos XG Firewall under **System > Administration > Time** and allow the correct network or the IP address of the RED.

Branch Name *	<input type="text"/>
Client Type	<input type="text" value="RED 10"/>
RED ID *	<input type="text"/>
Unlock Code *	<input type="text"/>
Firewall IP/Hostname *	<input type="text"/>
Description	<input type="text"/>
Device deployment	<input checked="" type="radio"/> Automatically via Provisioning Service <input type="radio"/> Manually via USB Stick

**Figure 95: Add RED Interface**

#### 4. Enter the details for Uplink Settings.

##### Uplink Connection

Select the connection type for the uplink:

- **DHCP:** The RED pulls an IP address from a DHCP server.
- **Static:** Enter an IP address, the corresponding netmask, a gateway and a DNS server IP address.

##### 2nd Uplink Connection (*available only if client Type is RED 50 is selected*)

Select the connection type for the uplink:

- **DHCP:** The RED pulls an IP address from a DHCP server.
- **Static:** Enter an IP address, a corresponding netmask, gateway and DNS server IP address.

##### 2nd Uplink Mode (*available only if client Type is RED 50*)

Select an uplink mode for the 2nd host.

- **Failover**
- **Load Balancing**

### 3G/UMTS Failover (*not available if Operation Mode is Transparent/Split*)

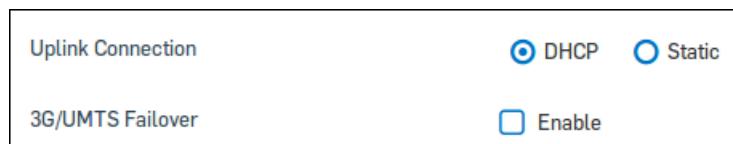
Select to enable the 3G/UMTS failover function. Clear the check box to disable the function.

 **Note:** Plug in a 3G/UMTS USB stick into the RED's USB port. The stick can provide Internet uplink failover in case of WAN interface failure. For the necessary settings refer to your Internet provider's data sheet.

- **Mobile Network:** Select the mobile network type from the drop-down list.
    - **GSM**
    - **CDMA**
  - **Username/Password** (*available only if CDMA is selected*): If required, specify a username and password for the mobile network.
  - **PIN** (*available only if GSM is selected*): Specify the PIN of the SIM card if a PIN is configured.
-  **Note:** If you specify a wrong PIN, the connection cannot be established through 3G/UMTS in case of WAN interface failure. Instead, the **3G/UMTS Failover** checkbox of the RED device is automatically cleared. Thus, the wrong PIN is used only once. When the WAN interface comes up again, the RED device displays a warning: *A wrong PIN was entered for 3G/UMTS failover uplink. Please change the login data..* When you open the **Edit RED** dialog box, a message is displayed which tells you that the 3G/UMTS failover was automatically unselected. Enter the correct PIN and select the checkbox. After making three connection attempts with a wrong PIN, the SIM card is locked. It cannot be unlocked through the RED device or Sophos XG Firewall and you have to contact the Sophos support.
- **APN** (*available only if GSM is selected*): Enter your provider's access point name information.
  - **Dial String**: If your provider uses a different dial string, enter it here.

Default for GSM: \*99#

Default for CDMA: #777



**Figure 96: RED Uplink Settings**

## 5. Specify the **RED Network Settings** details.

### RED Operation Mode

Select to define how the remote network is to be integrated into your local network:

- **Standard/Unified:** All the remote network traffic is routed through the Sophos XG Firewall which serves as the DHCP server and as the default gateway too. Sophos XG Firewall has complete control over the network traffic of the remote network. It can apply firewall rules to traffic between the local and remote LANs as well as filter web traffic and applications of the remote network.

 **Note:** Handle VLAN traffic through this mode if VLAN is deployed behind the RED.

- **Standard/Split:** Only traffic to select local networks is routed through the Sophos XG Firewall. Select the local networks from the drop-down list in the **Split Network** box or create new networks which can be accessed by the RED. Sophos XG Firewall controls the traffic to these

networks from the remote network. It also serves as the DHCP server and as the default gateway. All other remote network traffic is sent directly out through the local Internet connection.

 **Note:** VLAN tagged frames cannot be handled in this operation mode. To use a VLAN behind your RED device, select the Standard/Unified operation mode.

- **Transparent/Split** (*not available if 3G/UMTS Failover is selected*): Sophos XG Firewall does not control network traffic of the remote network, nor does it serve as the DHCP server nor as the default gateway. On the contrary, it pulls an IP address of the remote network from the DHCP server to become part of that network. However, you can enable access to the local network for remote clients. Define split networks that can be accessed by the remote network. Additionally, you can define one or more split domains to be accessible. If your local domains are not publicly resolvable, define a **Split DNS Server**, which can be queried by the remote clients.

 **Note:** VLAN tagged frames cannot be handled in this operation mode. To use a VLAN behind your RED device, select the Standard/Unified operation mode instead.

#### **RED IP** (*not available if Transparent/Split is selected*)

Enter the IP address of the RED device.

#### **RED Netmask** (*not available if Transparent/Split is selected*)

Select the netmask from the drop-down list.

#### **Zone**

Select the zone from the drop-down list:

- LAN
- DMZ
- VPN
- WiFi

#### **Configure DHCP**

Enable to configure a DHCP range for RED.

#### **RED DHCP Range** (*available only if Configure DHCP is selected*)

Enter the DHCP range which the RED is allowed to use.

#### **Split DNS Server** (*available only if Transparent/Split is selected*)

If your local domains are not publicly resolvable, you need to define a Split DNS Server, which can be queried by remote clients.

#### **Split Network** (*not available if Standard/Unified is selected*)

Select the split networks from the drop-down list or add more networks.

 **Note:** Traffic to the networks listed in the **Split Network** box is redirected to your Sophos XG Firewall. The remaining traffic is directly routed to the Internet.

To check traffic from the branch office to the main office intranet for viruses, route it through the Sophos XG Firewall. Or use the Sophos XG Firewall as an HTTP proxy.

#### **Split Domains** (*not available if Transparent/Split is selected*)

Add one or more split domains.

 **Note:** Since Sophos XG Firewall is only a client of the remote network, it is not possible to route traffic to the split networks the way it is done with the other modes. Therefore, the RED device intercepts all traffic: Traffic targeting to a network listed in the **Split Network** box or going to a domain listed in the **Split Domain** box is redirected to the Sophos XG Firewall interface. This is accomplished by replacing the default gateway's MAC address in the respective data packets with the MAC address of Sophos XG Firewall.

Example: A partner or service provider requires access to your intranet or a certain server in your local network. Using a RED device the partner's network remains completely independent of your network, but they can access a defined part of your network for certain purposes, as if they were connected via LAN.

### MAC Filtering Type

To restrict the MAC addresses allowed to connect to the RED device select **Blacklist** or **Whitelist**.

**Whitelist:** Only MAC addresses listed in the MAC Address list are allowed.

**Blacklist,** MAC addresses listed in the MAC address list are not allowed.

**MAC Address:** The list of MAC addresses used to allow or restrict access to the RED device. MAC address lists can be created on the **System > Hosts and Services > MAC Host** page.

 **Note:** MAC filtering only works for RED rev. 2 or newer. For RED 10, a maximum of 200 MAC addresses is allowed, whereas for RED 50, the list may contain up to 400 MAC addresses.

### Tunnel Compression

Select to compress all traffic sent through the RED tunnel. Data compression can increase the throughput of the RED device deployed in regions with very slow Internet connection such as 1-2 MBps. However, performance increase depends on the data's potential to be compressed (for example, data that is already compressed such as HTTPS or SSH cannot be compressed further). In some circumstances enabling data compression can actually reduce throughput of the RED device. In such case, disable data compression.

 **Note:** Tunnel compression is not available for RED 10 rev.1.

RED Operation Mode	<input checked="" type="radio"/> Standard/Unified <input type="radio"/> Standard/Split <input type="radio"/> Transparent/Split
RED IP *	<input type="text"/>
RED Netmask	<input type="text"/> /24 (255.255.255.0)
Zone	<input type="text"/> LAN
Configure DHCP	<input checked="" type="checkbox"/> ON
RED DHCP Range	<input type="text"/> <input type="text"/>
MAC Filtering Type	<input checked="" type="radio"/> None <input type="radio"/> Whitelist <input type="radio"/> Blacklist
Tunnel Compression	<input type="checkbox"/> Enable

**Figure 97: RED Network Settings**

- Enter the details of **Switch Settings** (available only if client Type is **RED 50**).

### Switchport Mode

RED 50 offers four LAN ports that can be configured either as simple switches or for intelligent VLAN usage. When set to Switch, all the traffic is sent to all ports. When set to VLAN, traffic can be filtered according to the Ethernet frames' VLAN tag, thus allowing the tunneling of more than one network into the RED tunnel.

Select the switchport mode for the switch settings

- Switch:** RED 50 uses the switch by default.

- **VLAN:** Select the LAN port(s) and enter the LAN VID(s).

When using the VLAN switch port configuration, you can configure each LAN port separately. For each LAN port, the following options are available:

- **Untagged (Hybrid Port):** Ethernet frames with the VLAN IDs specified in the LAN VID(s) field below will be sent to this port. The frames are sent without tags, thus the end devices do not have to support VLAN. This port allows just one VLAN ID.
- **Untagged, drop tagged (Access port):** Ethernet frames with the VLAN IDs specified in the LAN VID(s) field below will not be sent to this port. The frames are sent without tags, thus the end devices do not have to support VLAN.
- **Tagged (Trunk Port):** Ethernet frames with the VLAN IDs specified in the LAN VID(s) field below will be sent to this port. The frames are sent with tags, and the end devices have to support VLAN. Frames without VLAN IDs will not be sent to this port. This port allows up to 64 different VLAN ID(s) separated by comma.
- **Disabled:** This port is closed. No frames with or without VLAN IDs specified in the LAN VID(s) will be sent to this port.

## 7. Click **Save**.



**Note:** If the message “Registering with RED service failed. Please make sure that this device can connect to the Internet on port 3400” appears, a network problem has occurred. Check if you can reach `red.astaro.com` through port 3400 (via console command `telnet red.astaro.com 3400`). If you can, the error could be due to high network load. Retry to connect later.

## Related tasks

[Configure RED](#) on page 286

This page describes how to configure RED.

## Related information

[RED Supported 3G/4G/LTE USB Dongles](#)

## Manage RED Interface

This chapter describes the functions of the  icon of RED interfaces on the **Configure > Network > Interfaces** page.

The following options are available:

### Activate/deactivate

The toggle switch next to the branch name shows the status of the interface. Click it to turn it on/off.



**Note:** The RED interface is deactivated and can not be edited if the RED device is bound to another system.

### Download Provisioning file

This option is available only if the RED interface is in offline provisioning mode (if **Device Deployment** is set to **Manually via USB Stick**).

Clicking on the link will download the provisioning file for the RED device. Save the file to the root directory of a USB stick. Then plug the USB stick into the RED appliance before turning it on. The RED will fetch its configuration from the USB stick. After that the connection between your appliance and the RED appliance is going to be established.



**Note:** It is crucial that you keep the unlock code, which is emailed instantly to the address provided on the **RED Configuration** page as soon as the RED appliance receives its configuration. (In case of switching between manual and automatic deployment, make sure to keep both unlock codes.) You need the unlock code when you want to use the RED appliance with another Sophos XG Firewall. If you then do not have the unlock code ready, the only way to unlock the RED appliance is to contact the Sophos Support. The Support

however can only help you if you deployed the configuration automatically, via the RED Provisioning Service.

### **3G/UMTS Failover**

Displays if the **3G/UMTS Failover** function is enabled or disabled.

### **Configure RED Site-to-Site Tunnel**

This page describes how to set up a RED Site-to-Site Tunnel.

For such a connection, you need a RED server and a RED client. RED Site-toSite connection is also possible between Sophos XG Firewall and Sophos UTM using the RED server legacy and RED client legacy. For more information, see [RED Site-to-Site between Sophos XG Firewall and Sophos UTM](#) on page 126.

1. Configure the Firewall RED Server on the server machine.

How to configure RED is described in chapter [Configure RED](#) on page 286.

2. Add a RED interface on the **Interfaces** page.

How to add a RED interface is described in chapter [Add RED](#) on page 119.

3. Go to **Configure > Network > Interfaces**.

4. On the required RED interface, click the  icon towards the right and select **Download Provisioning File**.

5. Configure the Firewall RED Client on the client machine and upload the provisioning file you downloaded from the server machine.

The RED Site-to-Site tunnel has been established and is active. You can control the RED connection status on both machines in the **Network Security Control Center** in the section **User Threat Quotient**.

### *[RED Site-to-Site between Sophos XG Firewall and Sophos UTM](#)*

RED Site-toSite connection is also possible between Sophos XG Firewall and Sophos UTM. Select interface type **RED Server Legacy** if you want to use Sophos XG Firewall as a RED firewall server for a Sophos UTM client. The provisioning file needs to be uploaded in the Sophos UTM client management. When you use Sophos UTM as RED firewall you need to upload the provisioning file from the Sophos UTM in a Sophos XG Firewall interface with type **RED Client Legacy**.

#### Sophos XG Firewall as RED Firewall server

This page describes how to set up a RED Site-to-Site Tunnel between Sophos XG Firewall as RED firewall server legacy and Sophos UTM as RED client.

1. Ensure that RED on Sophos XG Firewall is activated. This can be done from **Configure > System Services > RED**.

2. Go to **Configure > Network**, click **Add Interface** on the upper right and select **Add RED** from the drop-down list.

3. Create a RED interface with type **RED Firewall Server Legacy**.

How to create a RED interface is described in chapter [Add RED](#) on page 119.

4. Download the provisioning file.

5. Log in to Sophos UTM.

6. Ensure that RED on Sophos UTM is activated. This can be done from **RED Management > Global Settings**.

7. Go to **RED Management > [Client] Tunnel Management**, click **New Tunnel**.

8. Create a tunnel and upload the provisioning file from Sophos XG Firewall.

How to create a tunnel is described in [Sophos UTM Administration Guide](#) (Chapter 15.5 Tunnel Management).

9. Go to **Interface & Routing > Interfaces**, click **New Interface**.

10. Create a interface with the RED tunnel.

How to create a RED interface is described in [Sophos UTM Administration Guide](#) (Chapter 6.1 Interfaces).

The Site-to-Site connection between Sophos XG Firewall and Sophos UTM is now activated and can be seen in SF-OS under **Configure > Network > Interfaces** and in the Control Center.

## Sophos UTM as RED Firewall Server

This page describes how to set up a RED Site-to-Site Tunnel between Sophos UTM as RED firewall server and Sophos XG Firewall as RED client legacy.

1. Ensure that RED on Sophos UTM is activated. This can be done from **RED Management > Global Settings**.
2. Go to **RED Management > [Server] Client Management**, click **New RED**.
3. Create a RED.  
How to create a RED is described in [Sophos UTM Administration Guide](#) (Chapter 15.3 Client Management).
4. Download the provisioning file.
5. Go to **Interface & Routing > Interfaces**, click **New Interface**.
6. Create an interface with the RED server.  
How to create a RED interface in Sophos UTM is described in [Sophos UTM Administration Guide](#) (Chapter 6.1 Interfaces).
7. Ensure that RED on Sophos XG Firewall is activated. This can be done from **Configure > System Services > RED**.
8. Go to **Configure > Network**, click **Add Interface** on the upper right and select **Add RED** from the drop-down list.
9. Create a RED interface with type **RED Firewall Client Legacy** and upload the provisioning file from Sophos UTM.  
How to create a RED interface is described in chapter [Add RED](#) on page 119.

The Site-to-Site connection is between Sophos XG Firewall and Sophos UTM is now activated and can be seen in SF-OS under **Configure > Network > Interfaces** and in the Control Center.

## Tap

The device provides seamless proof of concept through the Discover Mode, allowing you to evaluate its security performance prior to purchase. Through the Tap interface, Discover Mode enables you to monitor network traffic without making any change in the current network schema.

Connect the device to a switch through which all the network traffic passes. Configure the switch to forward a copy of every packet passing through it to the device. The device monitors the traffic passively and generates a Security Assessment Report (SAR) from the gathered data. SAR provides visibility into potential risks within the network, including application and web risks, risky users, intrusion risks, and more.



### Note:

- When deployed in Discover Mode, the device functions in listening mode. Hence, no firewall rule is applied.
- Only unbound physical interfaces can be configured in Discover mode.
- For interfaces configured in Discover Mode, the **Interfaces** page displays the zone name as **Discover**.
- The Tap interface cannot be updated or deleted.
- Subscription to Network Protection and Web Protection modules is required for the analysis of IPS, Web Filter and Application Filter policies.
- **Pre-requisites for Discover Mode:**
  - The device must be connected to the Internet for web classification, IPS updates and SAR generation in the cloud.
  - The device must be integrated with external authentication servers, such as Active Directory, RADIUS, LDAP etc., for the SAR to provide user-specific data.

## Enable Discover Mode

This page allows you to enable the Discover Mode through the Tap interface.

1. Access the CLI console by clicking **admin** on the upper right-hand corner of the Admin Console screen.
2. Select the option **Console**.

3. Provide the admin password.
4. Select the option **4. Device Console**.
5. Execute the following command to enable discover mode: `console> system discover-mode tap add <Port>`

```
console> system discover-mode tap add PortD
Discover Interface added successfully
console> █
```

**Figure 98: Enable Discover Mode**

The message “Discover Interface added successfully” is displayed on the CLI. Additionally, the interface configured in Discover Mode displays the message “Discover, Physical (Tap)” on the **Interfaces** page.

## Zones

This page displays a list of all the zones including system zones and lets you manage the zones.

A zone is a logical grouping of ports/physical interfaces and/or virtual sub-interfaces 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 writing the same policy for each interface.

Next to the **Name** of the zone type, the list displays the **Members** belonging to the specific zone, the zone **Type**, the kind of **Device Access** and, optionally, a **Description**.

### Default Zone Types

- **LAN** - Depending on the device in use and network design, you 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, it is the most secured zone. However, traffic between ports belonging to same zone with different networks will be allowed if the policy is applied for LAN to LAN.
- **DMZ (DeMilitarized Zone)** – This zone is normally used for publicly accessible servers. Depending on the device in use and network design, you can group multiple physical ports in this zone.
- **WAN** - This zone is used for Internet services. It can also be referred to 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, the port/interface used by the connection is automatically added to this zone and on disconnection; the 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.
- **WiFi** - This zone is used for wireless Internet services.

The device is shipped with a single zone for LAN, WAN, DMZ, VPN and WiFi. These zones are called system zones. Additionally, you can define LAN and DMZ zone types.

### Add Zone

1. Go to **Configure > Network > Zones** and click **Add**.
2. Enter the zone details.

#### Name

Enter a name to identify the zone.

#### Description

Enter the description for the zone.

#### Type

Select the type of zone from the available options. **LAN** - Depending on the device in use and network design, you 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, it is 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, you can group one to five physical ports in this zone.

 **Note:** By default, the entire traffic will be blocked except LAN to Local zone services like administration, authentication, and network.

## Members

Displays all the member ports.

Click the checkbox to select the ports. All the selected ports are moved to the ‘Selected port’ list.

## Device Access

Device access defines the type of administrative access permitted to a zone.

**Admin Services** - Enable administrative services that should be allowed through this zone:

- **HTTPS** - Allow secure HTTPS connection to the admin console through this zone
- **Telnet** – Allow Telnet connection to CLI through this zone
- **SSH** – Allow SSH connection to CLI through this zone

**Authentication Services** – Enable authentication services that should be allowed through this zone:

- Client Authentication
- Captive Portal
- NTLM
- Radius SSO

**Network Services** - Enable network services that should be allowed through this zone:

- DNS – Allow this zone to respond to DNS requests
- Ping/Ping6 – Allow this zone to respond to pings

**Other Services** - Enable other services that should be allowed through this zone:

- Web Proxy
- SSL VPN Tunnel
- Wireless Protection
- User Portal
- Dynamic Routing
- SNMP
- SMTP Relay

The screenshot displays the configuration interface for adding a new zone. The 'Name \*' field is labeled 'Enter Name'. The 'Description' field is labeled 'Enter Description'. Under 'Type \*', 'LAN' is selected. In the 'Members' section, 'None' is listed. The 'Device Access' section includes 'Admin Services' with checkboxes for HTTP, HTTPS, TELNET, and SSH. The 'Authentication Services' section includes checkboxes for Client Authentication, Captive Portal, NTLM, and Radius SSO. The 'Network Services' section includes checkboxes for DNS and Ping/Ping6. The 'Other Services' section includes checkboxes for Web Proxy, SSL VPN Tunnel, Wireless Protection, User Portal, Dynamic Routing, SNMP, and SMTP Relay.

**Figure 99: Add Zone**

3. Click Save.



**Note:**

- If DMZ uses a private IP address, use NATing to make them publicly accessible.
- Local and VPN zones cannot be updated or deleted.

The new zone has been created and appears on the **Zones** page.

## WAN Link Manager

A gateway routes traffic between the networks, and if the gateway fails, communication with an external network is not possible.

By default, the device supports only one gateway. However, to cope with gateway failure problems, the device provides an option to configure multiple gateways. But simply adding one more gateway is not an end to the problem. Optimal utilization of all the gateways is also necessary. The device's WAN Link Manager provides link failure protection by detecting the dead gateway and switching over to an active link. It also offers a mechanism to balance traffic between various links.

At the time of deployment, you have configured the IP address for a default gateway through the Network Configuration Wizard. You can change this configuration any time and configure additional gateways. You can use the WAN Link Manager to configure multiple gateways for load balancing and failover.

By default, all the gateways defined through the Network Configuration Wizard will be defined as "Active" gateway.

The device provides a powerful solution for routing and managing traffic across multiple Internet connections. Designed to provide business continuity for an organization of any size, the WAN Link Manager optimizes the use of multiple Internet links, such as T1s, T3s, DSL and cable connections from one or multiple Internet service providers. Capable of automatic failover in the event of link failure, it helps to assure that your network is always connected to the Internet.

It also gives you an option to configure multiple WAN interfaces to allow connecting your device to more than one Internet service provider (ISP).

When you configure multiple external interfaces, you even have an option to control which interface an outgoing packet uses.

## **Load Balancing**

Load balancing is a mechanism that permits to balance traffic between various links. It distributes traffic among various links, optimizing utilization of all the links to accelerate performance and cut operating costs. The device employs weighted round robin algorithm for load balancing to reach maximum utilization of the capacities across the various links.

Using link load balancing gives organizations the possibility to achieve:

- Traffic distribution that does not overburden any link
- Automatic ISP failover
- Improved user performance because of no downtime
- Increased bandwidth scalability

To achieve outbound traffic load balancing between multiple links:

- Configure links in active-active setup, defining gateways as Active
- Assign an appropriate weight to each gateway. Traffic is distributed across the links in proportion to the ratio of weights assigned to individual links.

## **How it works**

Load balancing is determined by the load metric. The load metric is weight. Each link is assigned a relative weight and the device distributes traffic across links in proportion to the ratio of weights assigned to individual links. This weight determines how much traffic will pass through a particular link in relation to the other link(s).

The administrator can set the weight and define how the traffic will be directed to providers to best utilize their bandwidth investments. Weight can be selected based on:

- Link capacity (for links with different bandwidths)
- Link/Bandwidth cost (for links with varying costs)

A weighted load balancing feature enables network managers to optimize network traffic and balance the load between multiple links/interfaces.

## **Gateway failover**

Gateway failover provides link failure protection so that when one link goes down; the traffic is switched over to the active link. This safeguard helps to provide uninterrupted, continuous Internet connectivity to users. The transition is seamless and transparent to the end user with no disruption in service and without downtime.

To achieve WAN failover between multiple links:

- Configure links in active-backup setup
- Define Active gateway/interface
- Define backup gateway/interface – Traffic through this link is routed only when the active interface is down
- Define failover rule

In the event of Internet link failure, the WAN Link Manager automatically sends traffic to available Internet connections without administrator intervention. If more than one link is configured as backup link, traffic is distributed among the links in the ratio of the weights assigned to them. On failover, the backup gateway can inherit the parent gateway's (active gateway) weight or can be configured.

The transition from the dead link to the active link is based on the failover rule defined for the link. The failover rule specifies:

- how to check whether the link is active or dead
- what action to take when a link is not active

The failover rule has the form:

IF Condition 1 AND/OR Condition 2 then Action

Depending on the outcome of the condition, traffic is shifted to any other available gateway.

A ping rule is automatically created for every gateway. The device periodically sends the ping request to check health of the link and if link does not respond, traffic is automatically sent through another available link. The selection of the gateway and how much traffic is to be routed through each gateway depends on the number of configured active and backup gateways.

## Gateway Failback

During a link failure, the device regularly checks the health of a given connection, assuring a fast reconnection as soon as the Internet service is restored. When the connection is restored and the gateway is up again, without the administrator's intervention, traffic is again routed through the active gateway. In other words, the backup gateway fails back on the active gateway.

## WAN Link Manager

The WAN Link Manager page displays a list of configured IPv4 and IPv6 gateways. The page also displays the status Active  or Deactive  for each gateway and failover rule in case multiple gateways are configured. You can change the gateway parameters, change the gateway status, add or remove the failover rule, and view the data transfer passed through the gateway.

For the backup gateway, the weight is NA while for the active gateway, the configured weight is displayed.

Click the data transfer icon  under the Manage column of the corresponding gateway to view the total data transferred through the gateway in graphical as well as in tabular form.

## Gateway Failover Timeout Configuration

### Gateway Failover Timeout

Configure the gateway failover timeout in seconds.

This is the time period the device waits before the gateway failover occurs.

Default: 60 seconds

Acceptable Range: 1 to 65535



Gateway Failover Timeout  seconds (1-65535)

**Apply**

**Figure 100: Gateway Failover Timeout Configuration**

## Update Gateway Configuration

1. Go to **Configure > Network > WAN Link Manager**, click the gateway's **Name** hyperlink or click the edit icon under the **Manage** column to edit its settings.
2. Enter the gateway details.

### Name

Enter the name of the gateway.

### IP Address

Enter the IP address assigned to the gateway.

### Interface

Specify the IP address of the interface.

#### Type

Specify the type of the gateway.

**Available Options:** **Active** - Traffic will route through the active gateway(s). If more than one active gateway is configured then the traffic will be load balanced between these gateways depending on the weight assigned to each gateway. **Backup** – A gateway used in an active/passive setup, where traffic is routed through the backup gateway only when the active gateway is down.

#### Weight

Depending on the weight, the gateway is selected for load balancing. The device distributes traffic across links in proportion to the ratio of weights assigned to individual links.

This weight determines how much traffic will pass through a particular link relative to the other link(s).

Gateways can be assigned a weight from 1 to 100.



**Note:** When multiple gateways are configured and one gateway goes down, the traffic is switched over to the available gateways according to the ratio of the weights assigned to the available gateways.

#### Default NAT Policy

Select the NAT policy to be used as default for a particular gateway.

By default, the MASQ NAT policy is configured.

Select **None**, if NAT should not be applied on that particular gateway.

Name *	gateway
IP Address *	1.15.1.1
Interface *	test-1.15.1.2/255.255.255.0
Type *	<input checked="" type="radio"/> Active <input type="radio"/> Backup
Weight *	1
Default NAT Policy *	MASQ

**Figure 101: Update Active Gateway Configuration**

- Enter the backup gateway details (*Only available, if the type is Backup*)

#### Activate This Gateway

Select gateway activation condition: automatically or manually.

#### Automatic failover

For automatic failover, activate the option **If ... Active gateway fails**.

From the dropdown list, specify when the backup gateway should take over from the active gateway. This takeover process will not require the administrator's intervention.

#### Available Options:

- Specific Gateway** - The dropdown list displays all configured gateways. The backup gateway will take over and traffic will be routed through the backup gateway only when the selected gateway fails.

- **ANY** – The backup gateway will take over and traffic will be routed through the backup gateway when any of the active gateway fails.
- **ALL** – The backup gateway will take over and traffic will be routed through the backup gateway when all the configured active gateways fail.

#### Manual failover

If you select **Manually**, the administrator will have to change the gateway manually when the active gateway fails.

#### Action on Activation

Configure weight for the backup gateway. The device distributes traffic across links in proportion to the ratio of weights assigned to individual link. This weight determines how much traffic will pass through a particular link relative to the other link.

#### Inherit weight of the failed active gateway

If this option is selected, the backup gateway will inherit the parent gateway's (active gateway) weight

#### Use configured weight

If this option is selected, the weight specified in the **Weight** field will be used for the backup gateway.

**Figure 102: Backup Gateway Details**

**4. Click Save.**

The gateway details have been updated.

**5. Configure the Failover Rules.**

#### IF Then Condition

From the dropdown list, select the communication protocol, such as **TCP** or **PING (ICMP)**. Select the protocol depending on the service to be tested on the host.

**Port:** For TCP communication, specify the port number for communication.

**on IP Address:** Specify the IP address of the computer or the network device which is permanently running or most reliable.

#### Condition

- **AND** - All the conditions must be satisfied before the specified action is taken
- **OR** - At least one condition must be satisfied before the specified action is taken.

A request is sent to an IP address. If the IP address does not respond to the request, the device considers the IP address as unreachable.

If ...

Not able to Connect PING Port \* on IP Address 1.15.1.1 AND

Not able to Connect TCP Port \* on IP Address \*

Then ...

'SHIFT to another available gateway'

**Figure 103: Configure Failover Rules**

6. Click Save.
- The failover rule has been updated.

### Add Failover Rule

1. Go to **Configure > Network > WAN Link Manager**, click the gateway's **Name** hyperlink or click the edit icon under the **Manage** column and click **Add** under the **Failover Rules** section.
2. Configure the failover rules.

#### IF Then Condition

From the dropdown list, select the communication protocol, such as **TCP** or **PING (ICMP)**. Select the protocol depending on the service to be tested on the host.

**Port:** For TCP communication, specify the port number for communication.

**on IP Address:** Specify the IP address of the computer or the network device which is permanently running or most reliable.

#### Condition

- **AND** - All the conditions must be satisfied before the specified action is taken
- **OR** - At least one condition must be satisfied before the specified action is taken.

A request is sent to an IP address. If the IP address does not respond to the request, the device considers the IP address as unreachable.

If ...

Not able to Connect PING Port \* on IP Address 1.15.1.1 AND

Not able to Connect TCP Port \* on IP Address \*

Then ...

'SHIFT to another available gateway'

**Figure 104: Configure Failover Rules**

3. Click Save.
- The failover rule has been added.

### Network Traffic Report for Default Gateway

Click the data transfer icon under the **Manage** column of the corresponding gateway to view the total data transferred through the gateway in graphical as well as in tabular form.

#### Network Traffic Report for Default Gateway Period

From the available options, select the period for the report of the network traffic that passed through the gateway.

#### Available Options:

- Weekly
- Monthly

- Custom

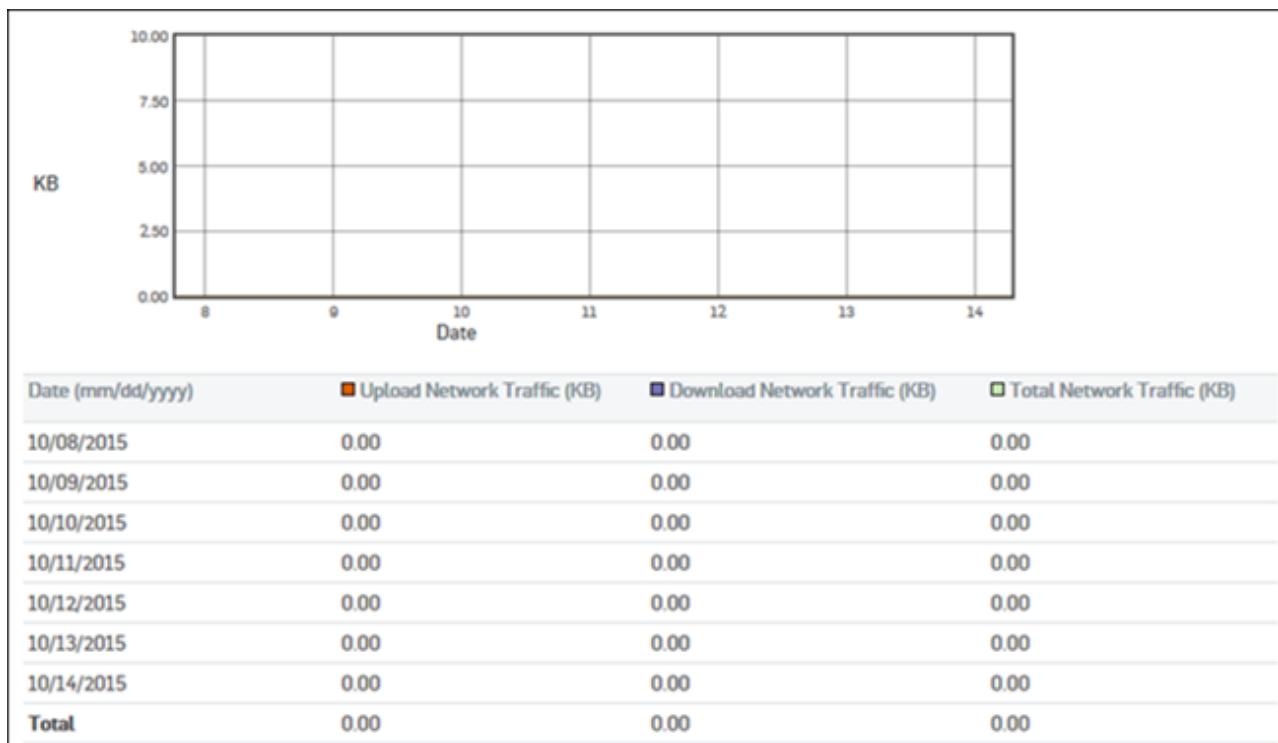
The graph displays the upload, download and total data transfer through the gateway.

- X-axis: Date (depending on the period selected)
- Y-axis: KB/MB/GB used

#### Legend

- Orange Color – Upload Network Traffic (MB)
- Purple Color – Download Network Traffic (MB)
- Green Color – Total Network Traffic (MB)

 **Note:** When the selected period is **Custom**, then the user can select to view data of not more than the last six (06) months. At one time, only thirty (30) days data will be displayed.



**Figure 105: Network Transfer Report**

## DNS

Use this page to configure the DNS settings of the device.

The DNS server is configured at the time of installation. You can add additional DNS servers to which the device can connect for name resolution. If multiple DNS are defined, they are queried in the order as they are entered.

 **Note:** You can also view and manage the DNS server status on the **Monitor & Analyze > Diagnostics > Services** page.

Sophos XG Firewall supports static DNS host entry where the device acts as a DNS Name Server that provides the requesting client with A records to resolve their requested URL.

You can manually add static DNS host entries for a particular domain name. Sophos XG Firewall checks DNS host entries for the requested domain name. If the domain name requested by the user matches the DNS host entry then the device performs DNS resolution and replies to the client with the IP address found in the static DNS host entry. DNS requests do not need to be redirected to the Local/Authoritative DNS server any longer. This facilitates faster data

transfer and avoids multiple DNS resolution cycles for every client request. You can also add multiple IP addresses for a single website hosted behind Sophos XG Firewall.

When you want external domains names to be resolved through internal DNS servers in your network, you can add DNS request routes to such servers. This will decrease the Internet traffic over the network and speed up DNS client requests as queries will not be forwarded outside the network. Also, DNS information would be less exposed on the Internet thus enhancing security.

## IPv4

### Obtain DNS from DHCP

Click to override the device DNS with the DNS address received from the DHCP server.

The option is available if enabled from the Network Configuration Wizard or if a DHCP interface is configured.

### Obtain DNS from PPPoE

Click to override the device DNS with the DNS address received from the PPPoE server.

The option is available if enabled from the Network Configuration Wizard or if a DHCP interface is configured.

### Static DNS

Select to provide a static IPv4 DNS server address.

A maximum of three static DNS IPv4 addresses can be provided.

<input type="radio"/> Obtain DNS from DHCP	
<input type="radio"/> Obtain DNS from PPPoE	
<input checked="" type="radio"/> Static DNS	
DNS 1	10.201.65.1
DNS 2	10.201.64.129
DNS 3	8.8.8.8

**Figure 106: IPv4 DNS Settings**

## IPv6

### Obtain DNS from DHCP

Click to override the device DNS with the DNS address received from the DHCP server.

The option is available if enabled from the Network Configuration Wizard or if a DHCP interface is configured.

### Static DNS

Select to provide a static IPv6 DNS server address.

A maximum of three static DNS IPv6 addresses can be provided.

The screenshot shows a configuration interface for IPv6 DNS settings. It includes three radio button options: 'Obtain DNS from DHCP', 'Obtain DNS from PPPoE', and 'Static DNS'. The 'Static DNS' option is selected. Below it, there are three input fields labeled 'DNS 1', 'DNS 2', and 'DNS 3', each containing an IP address: '10.201.65.1', '10.201.64.129', and '8.8.8.8' respectively.

**Figure 107: IPv6 DNS Settings****DNS Query Configuration****Choose server based on incoming requests record type**

Select to choose the DNS server to be used for resolving the domain name on the basis of the incoming requests record type. Incoming request can be of A or AAAA type.

**Choose IPv6 DNS server over IPv4**

Select to first choose the IPv6 DNS server for resolving the DNS and then the IPv4 DNS server.

If both IPv6 and IPv4 DNS servers are configured, then it first selects the IPv6 DNS server for all requests followed by the IPv4 DNS server.

**Choose IPv4 DNS server over IPv6**

Select to first choose the IPv4 DNS server for resolving the DNS and then the IPv6 DNS server.

If both IPv6 and IPv4 DNS servers are configured, then it first selects the IPv4 DNS server for all requests followed by the IPv6 DNS server.

**Choose IPv6 if request originator address is IPv6, else IPv4**

Select to choose the IPv6 DNS server if a request is received from an IPv6 source or choose the IPv4 DNS server, if a request is received from an IPv4 source.

**Apply**

Click to save the configuration.

**Test Name Lookup**

Click and provide an IP address or host name for testing the connectivity with the DNS server.

The screenshot shows a configuration interface for DNS query configuration. It includes four radio button options: 'Choose server based on incoming requests record type', 'Choose IPv6 DNS server over IPv4', 'Choose IPv4 DNS server over IPv6', and 'Choose IPv6 if request originator address is IPv6, else IPv4'. The first option is selected.

**Figure 108: DNS Query Configuration**

## DNS Host Entry

The **DNS Host Entry** section displays the list of all the configured host entries. You can filter the list based on the host/domain name. This section provides the option to add, update, or delete entries.

## DNS Request Route

This section displays a list of all the configured DNS request routes. You can filter the list based on the name or the target. Additionally, you can add, update and delete routes.

### Add DNS Host Entry

1. Go to **Configure > Network > DNS** and click **Add** under **DNS Host Entry** section.
2. Enter the host entry details.

#### Host/Domain Name

Provide a fully qualified domain name (FQDN) for the host/domain.

#### Address

Enter the address details for the host entry.

#### Entry Type

Select the DNS host entry type.

#### Available Options:

- Manual – Enter the IP address for the host manually
- Interface IP – Configure an interface as host

#### IP Address

Specify the IP address of the host/domain or select an interface IP depending on the option selected for the entry type.

Maximum entries per host: 8

#### Time to Live (seconds)

Specify the TTL in seconds.

Default: 60 seconds

#### Weight

Specify the weight for load balancing the traffic. The device distributes traffic across the links in proportion to the ratio of weights assigned to individual links.

This weight determines how much traffic will pass through a particular link relative to the other link(s).

Default: 1

#### Publish on WAN

Enable to publish the DNS host entry on WAN.

Default: Disabled

#### Reverse DNS Lookup

Reverse DNS lookup is the resolution of an IP address to its designated domain name. Enable to allow reverse DNS lookup.



**Note:** If there are multiple hosts resolving to the same IP address then **Reverse DNS Lookup** can only be configured for one of the IP addresses.

- Only A, AAAA, and PTR type of DNS records are supported.
- Address (A) record points a hostname to an IP address and returns a 32-bit IPv4 address.

- AAAA record points a hostname to an IP address and returns a 128-bit IPv6 address.
- Pointer records (PTR) are just the reverse of A records and are used for reverse lookups. They map the IP address to a hostname.
- Maximum DNS entries supported: 1024
- If the device interface is used as a DNS in the client system then a query is sent to the configured DNS servers prior to querying the ROOT servers.

Host/Domain Name \*

Address

Entry Type	IP Address	Time to Live (seconds)	Publish on WAN
Manual	192.168.1.100	60	Weight: 1

Reverse DNS Lookup  Add reverse DNS lookup for this Host entry

**Figure 109: DNS Host Entry**

3. Click Save.

The DNS host entry has been created and appears on the **DNS** page.

### Add DNS Request Route

1. Go to **Configure > Network > DNS** and click **Add** under **DNS Request Route** section.
2. Enter DNS request route details.

#### Host/Domain Name

Specify the domain for which you want to use the internal DNS server.

#### Target Servers

Select a DNS server(s) to resolve the domain specified above.

You can also add IP address to the DNS from this page by entering it in the entry field. Up to eight IP addresses can be added.

Host/Domain Name \*

Target Servers

Host List	Selected Host
<input type="text" value="type to search..."/>	
<input type="checkbox"/> RDP_Host	
<input type="checkbox"/> Gateway	
<input type="checkbox"/> My IP	
<input type="checkbox"/> 10.10.10.10	
<input type="checkbox"/> SNAT_IP	
<input type="checkbox"/> Web Server	

List order indicates priority

**Figure 110: Add DNS Request Route**

3. Click Save.

The DNS request route has been created and appears on the **DNS** page.

## DHCP

The **DHCP** section allows you to configure DHCP for your network.

On a network, the dynamic host configuration protocol (DHCP) automatically assigns IP addresses to the hosts on a network, thus reducing the administrator's configuration task. Instead of requiring administrators to assign, track and change (when necessary) IP addresses for every host on a network, DHCP settles it automatically. Furthermore, DHCP ensures that duplicate addresses are not used.

The **DHCP** section covers the following topics:

### Server

The device acts as a DHCP server: it assigns a unique IP address to a host and releases the address when the host leaves and re-joins the network. Each time, when the host connects to the network, it can have another IP address. In other words, the device provides a mechanism for allocating the IP address dynamically so that addresses can be re-used.

An interface having static IP assignment can also act as a DHCP server. You can disable or change this DHCP server configuration. You can configure IPv4 and IPv6 DHCP servers.

Using the **Server** section, you can configure, manage, and enable/disable DHCP servers on the device. It displays a list of all configured DHCP servers, and you can filter the list based on the IP family.



#### Note:

- The device cannot act as DHCPv6 server and DHCPv6 relay agent simultaneously.
- DHCPv4 Server and DHCPv4 Relay cannot be configured using the same Interface.

### Relay

Deploying DHCP in a single segment network is easy. All DHCP messages are IP broadcast messages, and therefore all the computers on the segment can listen and respond to these broadcasts. But things get complicated when there is more than one subnet on the network. The reason is that the DHCP broadcast messages do not cross the router interfaces by default. The DHCP relay agent makes it possible to place DHCP clients and DHCP servers on different networks. The relay agent allows DHCP broadcast messages to be sent over routers that do not support forwarding of these types of messages. The DHCP relay agent enables DHCP clients to obtain IP addresses from a DHCP server on a remote subnet, or from a server which is not located on the local subnet. If the DHCP relay agent is not configured, clients would only be able to obtain IP addresses from the DHCP server which is on the same subnet.

Using the **Relay** section, you can configure and manage DHCP relay agents on the device. It displays a list of all interfaces configured as a relay agent, and you can filter the list based on the relay agent name and the IP family.

### Lease

The device acting as a DHCP server assigns or leases an IP address from an address pool to a host DHCP client. The IP address is leased for a determined period of time or until the client relinquishes the address. The **IPv4/IPv6 Lease** section displays a list of all IPv4 and IPv6 addresses leased dynamically, and you can filter the lists based on the leased IP, or the client's physical address.

#### IPv4 Lease

For each IPv4 address, the list displays the following:

- Leased IP address
- Leased start and end time
- Client physical address
- Client host name
- Lease type

## IPv6 Lease

For each leased IPv6 address the list displays the following:

- Leased IP address
- Leased start and end time
- Client physical address
- DUID

### Related information

[Configure DHCP Options](#)

## Configure Interface as DHCPv4 Server

1. Go to **Configure > Network > DHCP**, click **Add** in the **Server** section and select **IPv4** using the default filter.
2. Specify the **General Settings** details.

### Name

Enter a name to identify the DHCPv4 server uniquely.

### Interface

Select an interface to set it as DHCPv4 server. DHCP service can be configured on a virtual interface but not on an interface alias.



**Note:** DHCPv4 Server and DHCPv4 Relay cannot be configured using the same Interface.

### Accept Client request via Relay

Select this to accept client requests through DHCP Relay.



**Note:** If you select this option, **Use Interface IP as Gateway** is disabled.

### Dynamic IP Lease

Specify the range of IP addresses from which the DHCP server must assign an IP address to the clients and set a subnet mask for the IP address range. You can configure multiple IP ranges for the same interface. Furthermore, you can provide multiple IP ranges for the DHCP server.

Click and to add or delete a range.

### Static IP MAC Mapping

If you want to assign specific IP addresses to some or all clients permanently, you can define static MAC address-to-IP address mappings. To define a MAC-IP mapping, you should know the MAC address of the client's network card. The MAC address is usually specified in hexadecimal digits separated by colons (for example, 00:08:76:16:BC:21). Specify the host name, the MAC address and the IP address. You can provide multiple MAC-IP mappings for the DHCP server.

Use and to add or delete a MAC-IP mapping.

### Subnet Mask

Select a subnet mask for the server.

### Domain Name

Specify the domain name that the DHCP server will assign to the DHCP clients.

### Gateway

Use this option to apply an interface IP as gateway.

Specify the IP address to be used as default gateway or select **Use Interface IP as Gateway** to use the IP address entered for **Interface**

### Default Lease Time

Specify the default lease time.

Acceptable range: 1 to 43200 minutes (30 days)

Default: 1440 minutes

#### Max Lease Time

Specify the maximum lease time. The DHCP client must ask the DHCP server for new settings after the specified maximum lease time has expired.

Acceptable range: 1 to 43200 minutes (30 days)

Default: 2880 minutes

#### Conflict Detection

Enable IP conflict detection to check the IP address before leasing. If enabled, the already leased IP address will not be leased again.

The screenshot shows the 'General Settings' configuration page. It includes fields for Name, Interface, and Accept Client request via Relay. Under Dynamic IP Lease, there are Start IP and End IP fields with a plus/minus button for adding rows. A note says '\* Press Tab to add a new row'. Under Static IP MAC Mapping, there are Hostname, MAC Address, and IP Address fields with a plus/minus button. A note says '\* Press Tab to add a new row'. Subnet Mask is set to /24 [255.255.255.0]. Domain Name and Gateway fields are present. Default Lease Time is set to 1440 (1-43200 Minutes [30 days]). Max Lease Time is set to 2880 (1-43200 Minutes [30 days]). Conflict Detection is set to Enable.

Name *	<input type="text" value="Enter Name"/>										
Interface	<input type="button" value="Select Interface"/>										
<input checked="" type="checkbox"/> Accept Client request via Relay											
Dynamic IP Lease	<table border="1"> <tr> <td>Start IP</td> <td>End IP</td> <td><input type="button" value="+"/></td> <td><input type="button" value="-"/></td> </tr> <tr> <td colspan="4">* Press Tab to add a new row</td> </tr> </table>	Start IP	End IP	<input type="button" value="+"/>	<input type="button" value="-"/>	* Press Tab to add a new row					
Start IP	End IP	<input type="button" value="+"/>	<input type="button" value="-"/>								
* Press Tab to add a new row											
Static IP MAC Mapping	<table border="1"> <thead> <tr> <th>Hostname</th> <th>MAC Address</th> <th>IP Address</th> <th><input type="button" value="+"/></th> <th><input type="button" value="-"/></th> </tr> </thead> <tbody> <tr> <td><input type="text"/></td> <td><input type="text"/></td> <td><input type="text"/></td> <td colspan="2">* Press Tab to add a new row</td> </tr> </tbody> </table>	Hostname	MAC Address	IP Address	<input type="button" value="+"/>	<input type="button" value="-"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	* Press Tab to add a new row	
Hostname	MAC Address	IP Address	<input type="button" value="+"/>	<input type="button" value="-"/>							
<input type="text"/>	<input type="text"/>	<input type="text"/>	* Press Tab to add a new row								
Subnet Mask *	<input type="text" value="/24 [255.255.255.0]"/>										
Domain Name	<input type="text"/>										
Gateway *	<input type="checkbox"/> Use Interface IP as Gateway <input type="text"/>										
Default Lease Time *	<input type="text" value="1440"/> 1-43200 Minutes [30 days]										
Max Lease Time *	<input type="text" value="2880"/> 1-43200 Minutes [30 days]										
Conflict Detection	<input type="checkbox"/> Enable										

**Figure 111: General Settings**

- Specify the DNS Server details.

#### Use Device's DNS Settings

Click to use the device's DNS server. In this case, the first two configured DNS will be used.

If not enabled, provide a primary and secondary DNS to be used.

#### Primary DNS (*available only if Use Device's DNS Settings is disabled*)

Specify the IP address of the primary DNS server.

#### Secondary DNS (*available only if Use Device's DNS Settings is disabled*)

Specify the IP address of the secondary DNS server.

<input type="checkbox"/> Use Device's DNS Settings	
Primary DNS	<input type="text"/>
Secondary DNS	<input type="text"/>

**Figure 112: DNS Server details**

4. Specify **WINS Server** details.

**Primary WINS Server**

Specify the IP address of the primary WINS server.

**Secondary WINS Server**

Specify the IP address of the secondary WINS server.

Primary WINS Server	<input type="text"/>
Secondary WINS Server	<input type="text"/>

**Figure 113: WINS Server details**

5. Click **Save**.
6. To enable or disable the DHCP server, go to **Configure > Network > DHCP** and turn the Status On or Off.

**Related information**

[Configure DHCP Options](#)

**Configure Interface as DHCPv6 Server**

1. Go to **Configure > Network > DHCP**, click **Add** in the **Server** section and select **IPv6** using the default filter.
2. Specify the **General Settings** details.

**Name**

Enter a name to identify the DHCPv6 server uniquely.

**Interface**

Select an interface to set it as DHCPv6 server. DHCP service can be configured on a virtual interface but not on an interface alias.

**Accept Client request via Relay**

Select this to accept client requests through DHCP Relay.

**Dynamic IP Lease**

Specify the range of IPv6 addresses from which the DHCP server must assign an IP address to the clients and set a subnet mask for the IPv6 address range. You can configure multiple IPv6 range for the same interface.

Furthermore, you can provide multiple IP ranges for the DHCP server.

Click  and  to add and delete a range.

**Static IP DUID Mapping**

If you want to assign specific IP addresses to some or all clients permanently, you can define static DUID address-to-IP address mappings. To define DUID-IP mapping, you should know the DHCP Unique Identifier (DUID) of the client. The DUID address is usually specified in groups of two hexadecimal digits separated by colons.

\*Each DHCP client and server has a DUID. DHCP servers use DUIDs to identify clients for the selection of configuration parameters. DHCP clients use DUIDs to identify a server in messages where a server needs to be identified.

Specify the host name, DUID and the IP address. You can provide multiple DUID-IP mappings for the DHCP server.

Click  and  to add or delete a DUID-IP mapping.

### Preferred Time

Specify the preferred time.

Acceptable range: 1 to 43200 minutes (30 days)

Default: 540 minutes

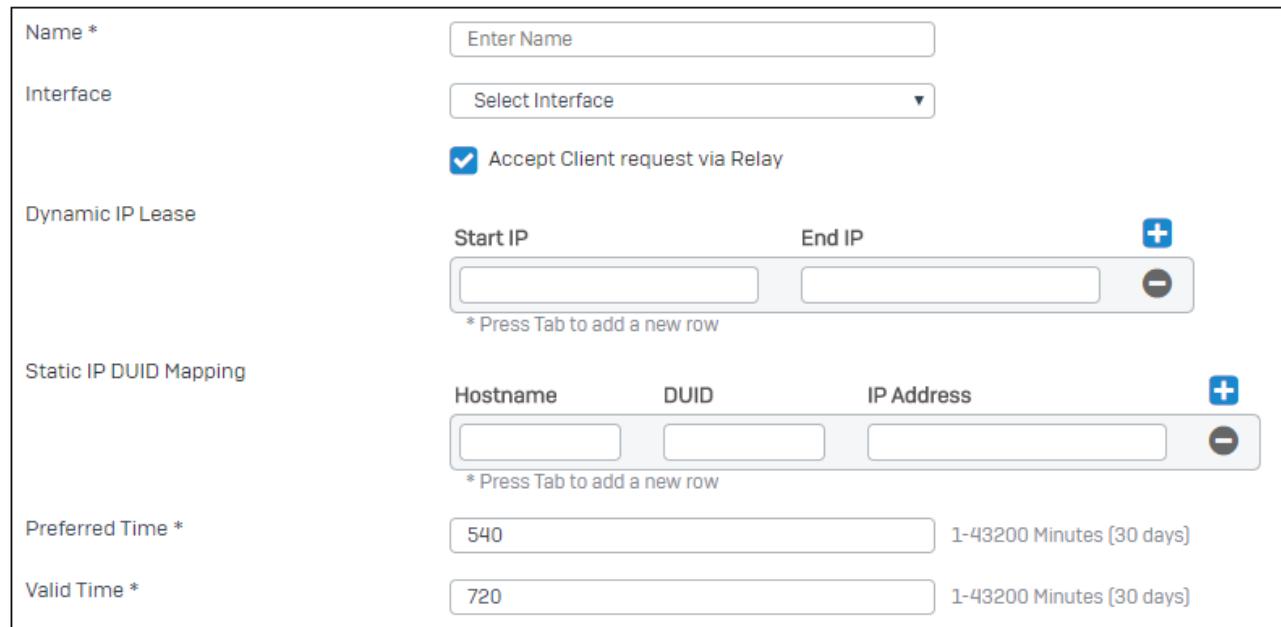
 **Note:** Preferred time should be less than valid time.

### Valid Time

Specify the valid time.

Acceptable range: 1 to 43200 minutes (30 days)

Default: 720 minutes



Name *	<input type="text" value="Enter Name"/>		
Interface	<input type="button" value="Select Interface"/>		
<input checked="" type="checkbox"/> Accept Client request via Relay			
Dynamic IP Lease	<input type="text" value="Start IP"/>	<input type="text" value="End IP"/>	
	 		
* Press Tab to add a new row			
Static IP DUID Mapping	<input type="text" value="Hostname"/>	<input type="text" value="DUID"/>	<input type="text" value="IP Address"/>
	 		
* Press Tab to add a new row			
Preferred Time *	<input type="text" value="540"/> 1-43200 Minutes [30 days]		
Valid Time *	<input type="text" value="720"/> 1-43200 Minutes [30 days]		

**Figure 114: General Settings**

- Specify the DNS Server details.

#### Use Device's DNS Settings

Click to use the device's DNS server. In this case, the first two configured DNS will be used.

If not enabled, provide a primary and secondary DNS to be used.

#### Primary DNS (*available only if Use Device' DNS Settings is disabled*)

Specify the IPv6 address of the primary DNS server.

#### Secondary DNS (*available only if Use Device' DNS Settings is disabled*)

Specify the IPv6 address of the secondary DNS server.

The screenshot shows a configuration interface for DNS server settings. At the top is a checkbox labeled "Use Device's DNS Settings". Below it are two sections: "Primary DNS" and "Secondary DNS", each with a corresponding empty input field.

**Figure 115: DNS Server details**

4. Click **Save**.
5. To enable or disable the DHCP server, go to **Configure > Network > DHCP** and turn the Status On or Off.

#### Related information

[Configure DHCP Options](#)

[\\* RFC 3315 \(Dynamic Host Configuration Protocol for IPv6 \(DHCPv6\)\)](#)

### Add DHCP Relay Configuration

1. Go to **Configure > Network > DHCP** and click **Add** in the Relay section.
2. Enter the DHCP relay configuration details.

#### Name

Provide a name to identify the DHCP relay agent.

#### IP Family

Select the IP family for the DHCP relay agent.

#### Available Options:

- IPv4
- IPv6

#### Interface

Select an interface on which your client network is configured. Device listens for DHCP queries on this interface and is used to forward packets between client and server.

Interfaces having a static IP assignment can act as a DHCP relay agent.

The DHCP relay agent can be configured on a virtual interface but not on an interface alias.



#### Note:

- The device cannot act as DHCPv6 server and DHCPv6 relay agent simultaneously.
- DHCPv4 Server and DHCPv4 Relay cannot be configured using the same Interface.

#### DHCP Server IP

Specify the DHCP server IP address. You can also configure multiple DHCP servers. This facilitates deploying DHCP servers in high availability environment. The DHCP relay will forward packets to all configured DHCP servers, and the active server will serve the request. In case the active server goes down, the backup server serves the request. The DHCP server takes care of leasing the IP address to a client.

Maximum DHCP servers configurable per DHCP relay: 8

#### Relay through IPSec (*Only available if IP family is IPv4*)

Select to relay DHCP messages through an IPSec VPN tunnel.

The screenshot shows a configuration interface for adding a DHCP relay. It includes fields for 'Name \*', 'IP Family \*' (with 'IPv4' selected), 'Interface \*' (a dropdown menu labeled 'Select Interface'), 'DHCP Server IP \*' (a search bar with a '+' icon), 'Relay Through IPsec' (a checkbox), and 'Enable' (another checkbox). The 'IP Family' section has radio buttons for 'IPv4' and 'IPv6'.

**Figure 116: Add DHCP Relay Configuration**

3. Click Save.

The DHCP relay agent has been created and appears on the **DHCP** page.

## IPv6 Router Advertisement

### Address Assignment for IPv6 Devices

IPv6 clients are assigned an IP address through:

- DHCP for IPv6
- Stateless address auto configuration (SLAAC)

### DHCP for IPv6

Similar to IPv4, IPv6 can use DHCP to assign IP addresses to any clients. The device can be configured to be a stateful DHCP server. The DHCP server is responsible for assigning the IP address to the client and for keeping a record of all clients and the IPv6 addresses assigned to them.

### Stateless Address Auto Configuration

The IPv6 protocol supports address auto configuration for stateless addresses. IPv6 devices automatically create unique link-local addresses for IPv6 enabled interfaces, and clients use router advertisement messages to configure their own IP address automatically.

### Router Advertisement

The device acting as a router has the ability to participate in stateless auto configuration (SLAAC) and by default provides a IPv6 address and a default gateway to the client.

When the device interface is connected to a network and enabled, the host may send out an ICMPv6 (type 135) Router Solicitation (RS) message that requests the device to generate Router Advertisement (RA) immediately instead of waiting until their next scheduled time. On receiving the RS message, the device immediately sends an ICMPv6 (type 134) router advertisement (RA) message announcing the state of its availability. Router advertisements include information about which method to be used for address assignment, prefixes used for on-link determination and/or address configuration, hop limit value, several flag status, etc. The critical parameters can be administered centrally and if necessary, can be propagated automatically to all hosts on the network. The device advertises information about various interfaces and Internet parameters either periodically or in response to the RS message, informing all the nodes on the network about any modification regarding addressing information. Thus, Router advertisement (along

with prefix flags) permits simple stateless auto configuration and guides a host in generating an address using auto-configuration.

-  **Note:** You can also view and manage the router advertisement service status on the **Monitor & Analyze > Diagnostics > Services** page.

## Configure IPv6 Router Advertisement settings

1. Go to **Configure > Network > IPv6 Router Advertisement** and click **Add**.
2. Enter details for the General Settings.

### Interface

Select an interface for router advertisement.

All IPv6 enabled physical interfaces, LAG, VLAN and bridge interfaces can be selected.

### Description

Enter a description for the interface to be selected for router advertisement.

### Min Advertisement Interval

Specify the minimum time interval in seconds between two consecutive unsolicited router advertisement messages sent to the clients.

Acceptable range: 3 to 1350 seconds

Default: 198 seconds

If the **Max Advertisement Interval** is 9 seconds or above, then the **Min Advertisement Interval** must be:  $0.75 * \text{maximum advertisement interval}$ .

### Max Advertisement Interval

Specify the maximum time interval in seconds between two consecutive unsolicited router advertisement messages sent to the clients.

Acceptable Range: 4 to 1800 seconds

Default: 600 seconds

### Managed Flag

Select to set the managed flag. When this flag is set, IPv6 addresses are obtained from the DHCPv6 server.

By default, this flag is not selected.

-  **Note:** The option must be selected only if a DHCPv6 Server is available else IPv6 clients would not get IPv6 addresses

### Other Flag

Select to set the other flag. When this flag is set, the DHCPv6 client obtains other network parameters such as DNS server, domain name, NIS, NISP, SIP, SNTP, and BCMS servers from the DHCPv6 server.

-  **Note:** This option must be selected only if a DHCPv6 server is available.

### Default Gateway

Select to use the device as default gateway for communication with the client.

### Life Time

Specify the time in seconds to be used for router advertisement as a default gateway at the client end.

The value specified should be between the value specified for **Max Advertisement Interval** and 9000 seconds.

Default: 1800 seconds

## Prefix Advertisement Configuration

Prefix Advertisement includes zero or more prefix options containing information that the default gateway advertises. This information is used by stateless address auto configuration to auto-generate a global IPv6 address. Prefix advertisement has its own list of attributes:

### **Prefix / 64**

Provide the first 64 bits of the IPv6 address.

The interface uses this prefix information from the router advertisement message to determine the last 64 bits (interface identifier) of its 128-bit IPv6 address.

The first 64 bits (higher order bits) of the IPv6 address so provided, specify the network, while the remaining specify a particular address in the network. Hence, IPv6 addresses in one network have the same first 64 bits and are called “prefix”.

### **On-link**

Select to set the prefix to be “On-link”. With the attribute **On-link** set, the devices with IPv6 addresses that are within this prefix are reachable on the subnet without a need of a router.

By default, this flag is set.

### **Autonomous**

Select to set the prefix attribute **Autonomous**. On being set, the global IPv6 address is automatically generated by appending the 64 bit interface identifier to the prefix (prefix /64) advertised in the prefix information.

Only those prefixes that has the **Autonomous** flag set gets a stateless address auto configuration (SLAAC) IPv6 address.

By default, the flag is set.

### **Preferred Life Time**

Specify the time in minutes for a valid address to remain in the preferred state. The use of the preferred address is unlimited.

On expiry of the valid life time, the preferred address becomes deprecated. The use of the deprecated address must be avoided, however, it is not forbidden and can be continued to be used as source address for an existing communication.

The IPv6 address will continue to remain in the preferred state as long as it is refreshed by prefixes in the router advertisement or by any other means or are renewed by DHCPv6.

Acceptable values: 0 to 71582789 minutes

Default: 240 minutes

Specify the attribute value as “-1” for an infinite preferred life time.

### **Valid Life Time**

Specify the time in minutes for an address to remain in the valid state.

This value determines the time for an address to be in the valid state. Until the time expires, the prefix is considered to be on-link and auto-configured addresses using the prefix can be used.

On expiry of the valid life time, the IPv6 address becomes invalid and cannot be used to send or receive traffic.

Acceptable range: 0 to 71582789 minutes

Default: 1440 minutes

Specify the attribute value as “-1” for an infinite valid life time.

Use the  and  icons to add or remove a prefix.

 **Note:** The value of attribute **Valid Life Time** must be greater than or equal to value of **Preferred Life Time**.

Prefix /64	On-link	Autonomous	Preferred Lifetime (Minutes, -1 for Infinite)	Valid Lifetime (Minutes, -1 for Infinite)
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	240	1440

**Figure 117: General Settings**

### 3. Enter the details for the Advanced Settings

Using the network discovery protocol (NDP) devices on the same interface discover the presence of each other and the respective link-layer addresses, find gateway routers and maintain the reachability information about the active paths to the peers.

#### Link MTU

Specify the Maximum Transmission Unit (MTU) in bytes for the packets sent on this interface.

Specify the Maximum Transmission Unit (MTU) in bytes for the packets sent on this interface.

Default: 0

Acceptable range: 1280 to 1500 bytes

If **Link MTU** is set to zero, the information will not be advertised by the interface.

#### Reachable Time

Specify the reachable time in seconds that the client will use to assume a neighbor is reachable after having received a reachability confirmation message.

Default: 0

Acceptable range: 0 to 3600 seconds

#### Retransmit Time

Specify the retransmission time in seconds that the client will use to determine how long it should wait before retransmitting neighbor solicitation messages.

Default: 0

Acceptable range: 0 to 4294968 seconds

#### Hop Limit

Specify the hop limit value.

This value determines the number of hops that a packet is limited to. The hop value is decremented by each router along the route. On reaching zero, the packet is destroyed.

Default: 64

Acceptable range: 0 to 255 seconds

Link MTU	<input type="text" value="0"/> (1280 to 1500 or 0)
Reachable Time	<input type="text" value="0"/> (0-3600 seconds)
Retransmit Time	<input type="text" value="0"/> (0-60 seconds)
Hop Limit	<input type="text" value="64"/> (0 - 255)

**Figure 118: Advanced Settings**

4. Click Save.

The IPv6 router advertisement settings have been updated.

## Cellular WAN

**This feature is not supported in Sophos Virtual Security Devices.**

Cellular WAN is a wide area network (WAN) for data that is typically provided by the cellular carriers to transmit a wireless signal over a range of several miles to a mobile device. Cellular WAN connectivity allows a user with a laptop and a Cellular WAN support to use the web, or connect to a VPN from anywhere within the regional boundaries of a cellular service.

Cellular WAN are popularly known as “wireless broadband”.

To configure Cellular WAN:

1. Enable Cellular WAN. You can also enable from CLI with the command: `system cellular_wan enable`.
2. Re-login to the Admin console.
3. Edit the Cellular WAN (WWAN1) interface and configure the Cellular WAN initialization string and gateway from **Configure > Network > Interfaces** page.

To configure Cellular WAN settings, please refer: [Configure Cellular WAN Settings](#) on page 109

Once Cellular WAN is enabled, an interface named WWAN1 is created and it is the member of the WAN zone.

As Cellular WAN interface is a member of WAN zone:

- All the services enabled for the WAN zone from the **Device Access** page are automatically applicable on WWAN1 connection too.
- All the firewall rules applied on WAN zone will be applied on Cellular WAN (WWAN1) interface.
- A default host named ##WWAN1 is created and firewall rules and VPN policies can be created for the default host.
- WWAN1 gateway is added as backup gateway
- When the Cellular WAN is disabled from CLI in the Cellular WAN menu, default host ##WWAN1 and Cellular WAN gateway options will be removed from the Admin Console.



### Note:

- Cellular WAN is not supported in bridge mode.
- DHCP server configuration is not supported for the Cellular WAN (WWAN1) interface.
- If backup of a device is taken on which Cellular WAN is enabled and restored on a device where it is not enabled, Cellular WAN configuration would still be visible.

## Status

The **Cellular WAN** page displays the status of the Cellular WAN connection. Along with details of the Cellular WAN connection, the page also provides the facility to connect and disconnect the Cellular WAN connection. Below are the screen elements with their description:

### Cellular WAN

Enable/Disable Cellular WAN.

Default - Disabled

### Connect/Disconnect Button

Click to connect or disconnect the Cellular WAN connection. This process may take some time.

### Status

Displays the status of the connection. Status messages can be of the following types:

#### Possible Status:

- Modem not supported
- No Modem plugged-in
- Connecting...
- Reconnecting
- Connected
- Disconnected

### Modem Name

Name of the modem.

### IP Address

IP address assigned to the device.

### Gateway IP

IP address assigned as the gateway.

### Bytes Uploaded

Number of bytes uploaded (in KB).

### Bytes Downloaded

Number of bytes downloaded (in KB).

### Time Duration

Time period since Cellular WAN is connected.

Format: HH:MM::SS

Wireless WAN	<input checked="" type="button"/> ON
Status	No modem plugged-in <input type="button"/> Connect
Modem Name	NA
IP Address	NA
Gateway IP	128.0.0.1
Bytes Uploaded	NA
Bytes Downloaded	NA
Time Duration	NA

**Figure 119: Status of the cellular WAN Connection**

## IP Tunnels

An IP tunnel is an Internet protocol network communications path between two networks. It is used to encapsulate one network protocol as a carrier for another network protocol. It is often used by two separate networks having a router with different network addresses for communication. The device supports IPv6 tunneling. Hence, IPv6 packets can be encapsulated in IPv4 headers using the IP Tunnel feature.

This page provides a list of all configured IP tunnels. The administrator can create and manage IP tunnels from this page.

### Add IP Tunnel

The **Add IP Tunnel** page allows you to create or edit an existing 6in4, 6to4, 6rd or 4in6 IP tunnel.

1. Go to **Configure > Network > IP Tunnels** and click **Add**.
2. Enter the tunnel details.

#### Tunnel Name

Enter a unique name to identify the tunnel.

#### Tunnel Type

Select the tunnel type from the available options.

#### Available Options:

- 6in4 – 6in4 uses tunneling to encapsulate IPv6 traffic over IPv4 links. This is used when IPv6 packets have to travel over IPv4 links with IPv6 networks at both endpoints..
- 6to4 – 6to4 allows encapsulation of an IPv6 packet in an IPv4 header to send it to an IPv4 destination. This is used when the local endpoint is an IPv6 host while the remote endpoint is an IPv4 host.
- 6rd – 6rd is similar in implementation to the 6to4 tunnel. However, unlike 6to4, 6rd allows the administrator to use a native IPv6 prefix.
- 4in6 – 4in6 uses tunneling to encapsulate IPv4 traffic over configured IPv6 tunnels. This is used when IPv4 traffic is to be used in a pure IPv6 network.

#### 6rd Prefix (available only if the tunnel type 6rd is selected)

Specify the native IPv6 prefix to be used for the tunnel.

#### Zone

Select the zone to create the tunnel for.

The tunnel is used for the traffic of the selected zone.

#### **Available Options:**

- LAN
- WAN
- DMZ
- WiFi

#### **Local Endpoint**

Specify the IP address of the local endpoint of the tunnel.

For:

- 6in4: Specify the IPv6 address of the local endpoint.
- 6to4: Specify the IPv6 address of the local endpoint.
- 6rd: Specify the IPv6 address of the local endpoint.
- 4in6: Specify the IPv4 address of the local endpoint.

#### **Remote Endpoint (available only if the tunnel types 6in4 or 4in6 are selected)**

Specify the IP address of the remote endpoint of the tunnel.

For

- 6in4: Specify the IPv4 address of the remote endpoint.
- 4in6: Specify the IPv6 address of the remote endpoint.

### **3. Enter the Advanced Settings.**

#### **TTL**

Specify the time to live (TTL) life time for the data.

The attribute **TTL** defines a limit regarding the number of attempts to transmit an IP packet before discarding it.

Default: 0

Acceptable Range: 0 to 255

#### **TOS**

Specify the type of service (TOS) for the data.

The attribute **TOS** provides the value for an IP packet depending on the service which is provided. The service mainly defines the packet priority, the type of route (latency, throughput, or reliable service).

Default: 0

Acceptable Range: 0 to 99

The form contains the following fields:

- Tunnel Name \***: An input field.
- Tunnel Type \***: A dropdown menu set to "Select Here".
- Zone \***: A dropdown menu set to "WAN".
- Local Endpoint \***: An input field.
- Remote Endpoint \***: An input field.
- Advanced Settings**: A link at the bottom right.

**Figure 120: IP Tunnel**

- Click Save.

The IP tunnel has been created or updated and appears on the **IP Tunnel** page.

## Neighbors (ARP-NDP)

From this page, view the IPv4 and IPv6 ARP-NDP neighbors, create static neighbors and flush existing neighbors.

### ARP-NDP

TCP/IP uses ARP (Address Resolution Protocol) protocol to translate an IPv4 address into a MAC address (physical network address). In other words, it maps layer 3 (IPv4 addresses) to layer 2 (physical or MAC addresses) to enable communications between hosts residing on the same subnet. Similarly to translate IPv6 addresses, NDP (Neighbor Discovery Protocol) is used.

ARP is used by hosts that are directly connected on a local network and uses either or both unicast and broadcast transmissions directly to each other. The host finds the physical address of another host on its network by sending an ARP query packet that includes the IP address of the receiver. As a broadcast protocol, it can create excessive amounts of network traffic on your network. To minimize the broadcast traffic, an ARP cache is maintained to store and reuse previously learned ARP information.

NDP in IPv6 is similar to ARP in IPv4. The main purpose of both protocols is to enable a host (node) to determine the link layer address (MAC address) of the node it wants to communicate with, in the local network and to find out the link layer address of the router through which it can access a node in an external network. Thus, the actual exchange of messages can take place between the two nodes. Apart from neighbor discovery, NDP functionality includes router discovery, neighbor presence, redirects, network options (as in DHCP options) and stateless auto-configuration.

Similar to ARP, NDP is also susceptible to flooding and poisoning attacks.

NDP has neighbor solicitations analogous to ARP request and neighbor advertisements analogous to ARP replies. Unsolicited neighbor advertisements in IPv6 correspond to gratuitous ARP replies in IPv4. Static neighbor configuration protects the neighbor cache from trusted or vulnerable nodes in the network. Static neighbor discovery helps to prevent solicit requests for configured entries and ignores any incoming solicit or advertised ND for configured entries.

### Neighbors

ARP and NDP traffic is a vital communication on a network and is enabled on the Device interfaces by default.

A static neighbor entry allows binding the MAC address to the designated IP address and port. Once the MAC address is bound to a port and IP address, the Device will not update its neighbor table dynamically and will not respond to that IP-MAC pair on any other port. It will also remove any dynamically cached references to that IP address that might be present, and will not allow additional static mappings of that IP address.

These entries will be stored in the **Static Neighbor Table**, the **IPv4 Neighbor Cache** and the **IPv6 Neighbor Cache**. The Device performs the neighbor lookup in the static neighbor table when it receives the request on a particular port. If there is any mismatch in an IP address or MAC address, the Device considers it as a neighbor poisoning attempt and does not update its neighbor cache. If an entry is not available in the table, the Device will lookup in the IPv4 or IPv6 neighbor cache and adds the MAC address to the neighbor cache if required.

Consider an example when IP1 is mapped to MAC1 and the IP1-MAC1 pair is bound to Port A. Similarly, IP2 is mapped to MAC1 and the IP2-MAC1 pair is bound to Port A

**Table 1: Illustration for Neighbor Poisoning**

IP Address	MAC Address	Port	Neighbor Poisoning Attempt
IP1	MAC1	A	No
IP1	MAC1	Any other port than A	Yes
IP1	MAC2	A	Yes
IP1	MAC2	Any other port than A	Yes
IP3	MAC1	No static ARP	No
IP2	MAC1	A	No
IP2	MAC1	Any other port than A	Yes

## Neighbors (ARP-NDP)

The device maintains three types of table for neighbor entries: Static Neighbor Table, IPv4 Neighbor Cache and IPv6 Neighbor Cache.

### IPv4/IPv6 Neighbor Cache table

The IPv4/IPv6 neighbor cache table stores static and dynamic neighbor entries. Static neighbor entries are defined by administrators and are permanent while dynamic neighbor entries are learned entries and are updated dynamically. Such dynamic entries can be flushed by clicking **Flush**.

Go to **Configure > Network > Neighbors (ARP-NDP)** and select **IPv4 Neighbor Cache** or **IPv6 Neighbor Cache** to view the large number of neighbor entries. This page allows navigating and managing the neighbor entries in all three tables. Select the table type from the drop-down list to view the neighbor entries in the respective table. It lists IP address, MAC address, interface and type of the entry. Entry type can be static or dynamic. If everything is working properly with the neighbor, the dynamic neighbor entry will be displayed as “Complete, Dynamic”. “Complete, Dynamic” means both MAC and IP values are there in the table while “Incomplete, Dynamic” means that the neighbor request was sent but no reply has yet been received.

## Neighbor Configuration

### Neighbor cache entry timeout

Specify time interval after which the entries in the cache should be flushed.

Default: 2 minutes

Input range: 1 to 500 minutes

Flush the IPv4/IPv6 neighbor cache whenever the host IP address on the network changes. As the IP address is linked to a physical address, it can change but can still be associated with the physical address in the IPv4/IPv6 Neighbor Cache. Flushing the IPv4/IPv6 Neighbor Cache allows new information to be gathered and stored in the IPv4/IPv6 Neighbor Cache.

### Log Possible Neighbor Poisoning Attempts

Enable to log the poisoning attempts.

Neighbor cache entry timeout  Minutes (1 - 500)

Log Possible Neighbor Poisoning Attempts

**Apply**

**Figure 121: Neighbor Configuration****Flushing Neighbor Table and Cache**

The neighbors page displays a list of all the IP address-and-MAC address mappings and you can filter the list based on the IP address or the MAC address.

Select **Static Neighbor Table** or the required cache and click the **Flush** button to empty the cache or click **Add** to add a new entry.

<input type="checkbox"/>	IP Address	MAC Address	Interface	Type	Manage
<input type="checkbox"/>	10.200.97.16	0a:12:5a:5b:26:96	PortB	Complete,Dynamic	
<input type="checkbox"/>	192.168.1.41	-	PortC	Incomplete	
<input type="checkbox"/>	10.200.97.35	ec:f4:bb:54:72:b0	PortB	Complete,Dynamic	
<input type="checkbox"/>	10.200.97.12	0e:1a:5a:5b:26:b0	PortB	Complete,Dynamic	
<input type="checkbox"/>	10.200.97.43	0a:12:5a:5b:27:51	PortB	Complete,Dynamic	
<input type="checkbox"/>	10.200.97.6	16:2a:5a:5b:10:69	PortB	Complete,Dynamic	
<input type="checkbox"/>	10.200.97.5	0a:12:fe:98:e0:11	PortB	Complete,Dynamic	
<input type="checkbox"/>	10.200.97.3	cc:4e:24:cf:66:80	PortB	Complete,Dynamic	
<input type="checkbox"/>	10.200.97.20	0e:1a:5a:5b:26:89	PortB	Complete,Dynamic	
<input type="checkbox"/>	1.15.1.1	-	test	Incomplete	
<input type="checkbox"/>	10.200.97.2	cc:4e:24:ce:f0:00	PortB	Complete,Dynamic	
<input type="checkbox"/>	10.200.97.1	02:e0:52:0f:ed:61	PortB	Complete,Dynamic	

**Figure 122: Neighbors****Add Static Neighbor**

1. Go to **Configure > Network > Neighbors (ARP-NDP)**. In Show section select **Static Neighbor Table** and click **Add**.
2. Specify the details.

**IP Family**

Select the IP Family for the static neighbor.

**Available Options:**

- IPv4
- IPv6

**IPv4/IPv6 Address**

Specify a IPv4/IPv6 address of the host outside the firewall.

**MAC Address**

Specify a MAC address of the host.

**Interface**

Select the physical interface on which the binding is to be done.

**Add as a Trusted MAC Address to prevent a spoofing attempt**

On enabling this option, the IP-MAC pair is added to the Trusted MAC list. If disabled, the IP-MAC pair will not be included in the Trusted MAC list.

By default, this option is enabled.

The screenshot shows a configuration interface for a static neighbor. At the top, there are two radio buttons: 'IPv4' (selected) and 'IPv6'. Below them are three input fields with asterisks: 'IPv4 Address' with placeholder 'Enter IP Address', 'MAC Address' with placeholder 'Enter MAC Address', and 'Interface' with placeholder 'Select Interface'. At the bottom is a checked checkbox labeled 'Add as a trusted MAC address to prevent a spoofing attempt'.

**Figure 123: Static Neighbor**

3. Click **Save**.

The static neighbor is created and appears in the **Static Neighbor Table** on the **Neighbors (ARP-NDP)** page.

**Dynamic DNS**

This section allows you to configure Dynamic DNS settings for your device.

Dynamic DNS (Domain Name Service) is a method of keeping a static domain/host name linked to a dynamically assigned IP address allowing your server to be more easily accessible from various locations on the Internet.

Powered by Dynamic Domain Name System (DDNS), you can access your device by the domain name, not the dynamic IP address. DDNS will tie a domain name (for example, mydevice.com, or mycompany.mydevice.com) to your dynamic IP address.

The device supports the following Dynamic DNS providers:

1. DynDNS
2. ZoneEdit
3. EasyDNS
4. DynAccess
5. Sophos

The page displays a list of all the configured DDNS, along with their names, interfaces, service providers, the last updated IP, status and time as well as the reason for failure. In addition it provides the option to add, update or delete a configuration.

## Add Dynamic DNS

This page describes how to either add details of a third-party DDNS provider or to configure the device itself to act as a DDNS.

Dynamic DNS cannot be configured from Sophos Firewall Manager (SFM).

1. Go to **Configure > Network > Dynamic DNS** and click **Add**.

2. Specify the DDNS parameter details.



**Note:** For configuring a third-party service provider, you need a registered account with any of the supported Dynamic DNS service providers:

1. DynDNS
2. ZoneEdit
3. EasyDNS
4. DynAccess
5. Sophos

### Hostname

Specify a name to identify the host that you want to use on the DDNS server. It is the domain name that you registered with your DDNS service provider, for example sophos.com.

In case you are configuring DynAccess as a service provider, provide the host name in the following format: <accountname>.dynaccess.com.

In case you are configuring Sophos as a service provider, provide the host name in the following format: <host\_name>.myfirewall.co.



**Note:** You cannot add DDNS provider as <host>.ddns.cyberoam.com.

### Interface

Select the external interface. The IP address of the selected interface will be bound to the specified hostname.

### IPv4 Address

Select the IPv4 address source.

Available Options:

- **Use Port IP:** Select to use the IP address of the selected port or interface.
- **NATed Public IP:** Select to use the public IP address assigned to the selected port.

### IP Edit Checking Interval

Specify the time interval after which the device should check and edit the IP address of your server, if changed.

Acceptable range: 4 - 60 minutes

Default: 20 minutes

For example, if the time interval is set to 10 minutes, after every 10 minutes, the device will check for any changes in your server IP address.

The screenshot shows the 'Host Details' configuration page. It includes fields for 'Hostname \*' (with a placeholder '(Example:xyz.dyndns.com)'), 'Interface \*' (a dropdown menu labeled 'Select Interface'), 'IPv4 Address \*' (radio buttons for 'Use Port IP' and 'NATed Public IP', with 'Use Port IP' selected), and 'IP Edit Checking Interval \*' (a numeric input field set to '20' with a range of '4-60 minutes').

**Figure 124: Host Details**

- Specify the Service Provider's Details.

#### Service Provider

Select the service provider with whom you have registered your hostname. In case you are configuring Sophos as a service provider, login name and password are not required.

#### Login Name

Specify your DDNS account's username.

In case you are configuring DynAccess as a service provider, provide the host name in the following format: <accountname>.dynaccess.com.

Provide your login name as <accountname>.

#### Password

Specify your DDNS account's password.

The screenshot shows the 'Service Provider Details' configuration page. It includes fields for 'Service Provider \*' (a dropdown menu labeled 'Select Service Provider'), 'Login Name \*' (a text input field containing 'admin'), and 'Password \*' (a text input field showing five asterisks).

**Figure 125: Service Provider Details**

- Click Save.

**Note:** You can configure multiple hosts having the same interface and service provider for Dynamic DNS.

## Authentication

---

The Authentication menu provides basic authentication settings for the device.

This menu covers the following topics:

- [Servers](#) on page 161: Manage external servers for authentication
- [Services](#): Define authentication servers for the administrators and end-users logging in through the device, VPN, or the Captive Portal.
- [Groups](#) on page 178: Set up policies and assign them to a number of users
- [Users](#) on page 182: Manage user accounts for access to the device

- [One-Time Password](#): Configure the one-time password (OTP) service.
- [Captive Portal](#) : Customize Captive Portal through which users can log in
- [Guest Users](#) on page 195: Manage users accessing the device without user account
- [Clientless Users](#) on page 201: Manage user accounts for clientless access
- [Guest User Settings](#) : Configure general parameters to provide secured Internet access for guest users
- [Client Downloads](#) on page 209: Download clients from different platforms to interact with the device

## Servers

The **Authentication Server** menu allows the management of databases and backend servers for external user authentication services.

External user authentication enables you to validate user accounts against existing user databases or directory services on other servers of your network.

Authentication services currently supported are:

- Novell's eDirectory
- Microsoft's Active Directory
- RADIUS
- TACACS+
- LDAP

This page displays a list of all existing authentication servers. For each server the list shows:

### Name

Displays the name of the authentication server.

### IP

Displays the IP address of the authentication server.

### Port

Displays the port of the authentication server.

### Type

Displays the type of the authentication server.

### Domain/Admin

Displays the domain or admin of the authentication server.

### Add External Server

This page describes the authentication servers to be added. It covers the following topics:

#### Active Directory

Active Directory (AD) is Microsoft's implementation of a directory service and is a central component of Windows 2000/2003 servers. It stores information about a broad range of resources residing on a network, including users, groups, computers, printers, applications, services, and any type of user-defined objects. As such it provides the means of centrally organize, manage, and control access to these resources. The Active Directory authentication method allows you to register Sophos XG Firewall at a Windows domain, thus creating an object for Sophos XG Firewall on the primary domain controller (DC). Sophos XG Firewall is then able to query user and group information from the domain.



**Note:** Sophos XG Firewall supports Active Directory 2003 and newer.

[Add Active Directory Server](#) on page 164

#### LDAP

LDAP, an abbreviation for Lightweight Directory Access Protocol, is a networking protocol for querying and modifying directory services based on the X.500 standard. Sophos XG Firewall uses the LDAP protocol to

authenticate users for several of its services, allowing or denying access based on attributes or group memberships configured on the LDAP server.

[Add LDAP Server](#) on page 162

## RADIUS

RADIUS, the acronym of Remote Authentication Dial In User Service, is a widespread protocol for allowing network devices such as routers to authenticate users against a central database. In addition to user information, RADIUS can store technical information used by network devices, such as supported protocols, IP addresses, routing information, and so on. This information constitutes a user profile, which is stored in a file or database on the RADIUS server. The RADIUS protocol is very flexible, and servers are available for most operating systems. The RADIUS implementation on Sophos XG Firewall allows you to configure access rights on the basis of proxies and users. Before you can use RADIUS authentication, you must have a running RADIUS server on the network. Whereas passwords are encrypted using the RADIUS secret, the username is transmitted in plain text.

[Add RADIUS Server](#) on page 167

## TACACS+

TACACS+, the acronym of Terminal Access Controller Access Control System, is a proprietary protocol by Cisco Systems, Inc. and provides detailed accounting information and administrative control over authentication and authorization processes. Whereas RADIUS combines authentication and authorization in a user profile, TACACS+ separates these operations. Another difference is that TACACS+ utilizes the TCP protocol (port 49) while RADIUS uses the UDP protocol.

[Add TACACS+ Server](#) on page 168

## eDirectory

Novell eDirectory is an X.500 compatible directory service for centrally managing access to resources on multiple servers and computers within a given network. eDirectory is a hierarchical, object-oriented database that represents all the assets in an organization in a logical tree. Those assets can include people, servers, workstations, applications, printers, services, groups, and so on.

[Add eDirectory Server](#) on page 169

### Add LDAP Server

This page describes how to add a LDAP server.

1. Go to **Configure > Authentication > Servers** and click **Add**.
2. As **Server Type**, select **LDAP Server**.
3. Specify the LDAP server details:

#### Server Name

Specify a descriptive name for the LDAP server.

#### Server IP/Domain

Specify an IP address or domain for the LDAP server.

#### Port

Specify the port of the LDAP server.

Default: 389

#### Version

Select the version of the LDAP server.

Default: 3

#### Anonymous Login

Enable to send anonymous requests to the LDAP server.

Disable to bind user with the server.

#### **Username (*not available if Anonymous Login is selected*)**

Enter user name. The username must be specified as a full distinguished name (DN) in LDAP notation, using commas as delimiters (e.g., uid=root,cn=user).

#### **Password (*not available if Anonymous Login is selected*)**

Specify a password for the user.

#### **Connection Security**

Select the connection security for the LDAP server:

- **Simple:** User credentials will be send unencrypted, as plaintext. This connection security is selected by default.
- **SSL:** Secure Sockets Layer. This is the most common method used for secured connection. The Port will then change from 389 (LDAPClosed) to 636 (ldaps = LDAP over SSL).
- **TLS:** Transport Layer Security. Same secure connection as SSL but uses the default port.

#### **Validate Server Certificate (*not available for Simple connection security*)**

Enable to validate the certificate on the external server.

#### **Client Certificate (*not available for Simple connection security*)**

Select a client certificate from the list to establish a secured connection. If you do not want a client certificate, select **None**.

Default: **ApplianceCertificate**



**Note:** You can manage client certificates under **Protect > Web Server > Certificates**.

#### **Base DN**

Enter the Base DN for the LDAP server. The Base DN is the starting point relative to the root of the LDAP tree where the users are included who are to be authenticated. Note that the Base DN must be specified by the Fully Distinguished Name (FDN) in LDAP notation, using commas as delimiters (e.g., O=Example,OU=RnD).

#### **Get Base DN**

Click **Get Base DN** if you are not aware about the Base DN. The Base DN is automatically retrieved from the directory.

#### **Authentication Attribute**

Specify an authentication attribute for searching the LDAP directory. The user authentication attribute contains the actual login name each user is prompted for, for example by remote access services.

#### **Display Name Attribute**

Specify the name for the LDAP server which is displayed as LDAP username.

#### **Email Address Attribute**

Specify the alias for the configured email address which is displayed to the user.

#### **Group Name Attribute**

Specify the alias for the configured group name which is displayed to the user.

#### **Expiry Date Attribute**

Specify the user expiry date displayed to the user. The attribute specifies how long a user account is valid.

Server Type	<input type="text" value="LDAP Server"/>
Server Name *	<input type="text" value="Enter Server Name"/>
Server IP/Domain *	<input type="text" value="Enter Server IP"/>
Port *	<input type="text" value="389"/>
Version *	<input type="text" value="3"/>
Anonymous Login *	<input checked="" type="checkbox"/>
Connection Security *	<input type="text" value="Simple"/>
Base DN *	<input type="text" value="Enter Base DN"/> <a href="#" style="color: blue; text-decoration: none;">Get Base DN</a>
Authentication Attribute *	<input type="text" value="Enter Authentication Attribute"/>
Display Name Attribute	<input type="text" value="Enter Display Name Attribute"/>
Email Address Attribute	<input type="text" value="mail"/>
Group Name Attribute *	<input type="text" value="Enter Group Name Attribute"/>
Expiry Date Attribute *	<input type="text" value="Enter Expiry Date Attribute"/>

**Figure 126: Add LDAP Server**

4. Click **Test Connection** to check the connectivity between LDAP and Sophos XG Firewall. It also validates the LDAP server user credentials.
5. Click **Save**.

### Add Active Directory Server

This page describes how to add an Active Directory server.

Active Directory allows the device to map the users and groups from ADS for the purpose of authentication on a Windows platform.

1. Go to **Configure > Authentication > Servers** and click **Add**.
2. As **Server Type**, select **Active Directory**.

 **Note:** If a user is required to authenticate using AD, the device needs to communicate with the AD server for authentication.

3. Specify the Active Directory server details.

#### Server Name

Enter a unique name for the Active Directory server.

#### Server IP

Specify an IP address for the Active Directory server.

#### Port

Specify the port of the Active Directory server.

Default: port 389.

#### NetBIOS Domain

Specify a NetBIOS domain for the Active Directory server.

#### ADS Username

Specify a username for the admin user of the Active Directory server.

#### Password

Specify a password for the admin user of the Active Directory server.

#### Connection Security

Select the type of security to be implemented on the established connection.

It provides a method to login to the external server by sending the username and password in encrypted format instead of plaintext.

- **Simple:** User credentials will be send unencrypted as plaintext.
- **SSL:** Secure Sockets Layer. This is the most common method used for secured connection. The Port will then change from 389 (LDAPClosed) to 636 (ldaps = LDAP over SSL).
- **TLS:** Transport Layer Security. Same secure connection as SSL but uses the default port.



**Note:** We strongly recommend using the encryption method to protect the user credentials.

#### Validate Server Certificate (*not available for Simple connection security*)

Enable to validate the certificate on the external server.

#### Display Name Attribute

Specify the name for the AD server which is displayed as AD username.

#### Email Address Attribute

Specify the alias for the configured email address which is displayed to the user.

#### Domain Name

Specify the domain name for which the query is to be added.

#### Search Queries

Click **Add** to enter the search query. Use the **Move Up** and **Move Down** buttons to rearrange the search queries in the list. Use **Remove** to remove the selected item.



**Note:** If you do not know the search DN, refer to [NetBIOS name, FQDN and Search DN](#).

Server Type: Active Directory

Server Name \*: MyServerName

Server IP \*: Enter Server IP

Port \*: 389

NetBIOS Domain \*: Enter NetBIOS Domain

ADS Username \*: admin

Password \*: \*\*\*\*

Connection Security \*: Simple

Display Name Attribute: Enter Display Name Attribute

Email Address Attribute: mail

Domain Name \*: Enter Domain Name

Search Queries \*: (empty list)

Add  
Remove  
Move Up  
Move Down

**Figure 127: Add Active Directory Server**

- Click **Test Connection** to check the connectivity between the Active Directory server and Sophos XG Firewall. It also validates the Active Directory server user credentials.
- Click **Save**.

***NetBIOS Name, FQDN and Search DN***

This page describes how a Search DN is built.

The settings have to be performed on an AD (Windows) server.

- Go to **Start > All Programs > Administrative Tools > Active Directory Users and Computers**.
- Right-click the required domain and go to the **Properties** tab.

Search DN is based on the FQDN. For example, if the FQDN is “google.com”, then the Search DN will be DC=google, DC=com.

Search Query

Search Query \*: Enter Search Query

Add Cancel

**Figure 128: Search Query*****Import AD User Group***

This page describes how to import Active Directory groups from the Windows platform into the device.

1. Go to **Configure > Authentication > Servers** and click  against the AD server from which AD groups are to be imported.  
The **Import Group Wizard Help** appears.
2. Specify a Base DN. Appliance fetches AD groups or OU groups from the specified Base DN.
3. Select the AD groups or OU groups to be imported in the appliance. Hold down **Ctrl** to select multiple groups. The appliance already available in the device will not be imported.
4. Select various policies (surfing quota, traffic shaping, web filter, application filter, network traffic and SSL VPN) and user authentication timeout group members. Selected policies are attached to all imported groups. If you want to specify different policies for different groups, do not enable the policy. For example if you want to specify different Internet policies to filter policies to different groups, do not enable **Attach to all the Groups**.
5. If you do not want to apply common policies which are valid for all groups, specify policies to be applied to each group individually.  
If groups are imported successfully, a “successful” message will be displayed; else the appropriate error message will be displayed. This message remains even if you close the wizard.
6. Click **Close** to end the wizard.

If a user is member of multiple AD groups, then the policies are applied to the first group the user is member of. Therefore, the device browses through the group ordered list from top to bottom to determine the user’s group membership. The first group that matches is considered the group of the user and that group policies are applied to the user.

Using the wizard, you can reorder the groups to change the membership preference.

## Add RADIUS Server

This page describes how to add a RADIUS server.

1. Go to **Configure > Authentication > Servers** and click **Add**.
2. As **Server Type**, select **RADIUS Server**.
3. Specify the RADIUS server details:

### Server Name

Specify a descriptive name for the RADIUS server.

### Server IP

Specify an IP address for the RADIUS server.

### Authentication Port

Specify the authentication port of the RADIUS server.

By default, this is port 1812.

### Enable Accounting

Enable accounting on the RADIUS server.

Sophos XG Firewall sends the following information to the RADIUS server as soon as the user logs in:

- Accounting start request
- User login time

Sophos XG Firewall sends the following information to the RADIUS server the moment the user logs out:

- Accounting stop request
- User logout time

 **Note:** Supported client types: Windows client, HTTP client, Linux client, Android, iOS, iOS HTTP client, Android HTTP client, API client.



**Note:** The accounting stop message is not sent to the RADIUS server when Sophos XG Firewall shuts down or reboots.

#### Accounting Port (*available only if Enable Accounting is active*)

Specify a RADIUS port number through which Sophos XG Firewall can communicate with the RADIUS server.

#### Shared Secret

Specify the shared secret which is a text string that serves as a password between a RADIUS client and a RADIUS server.

#### Group Name Attribute

Specify the alias for the configured group name which is displayed to the user.

Server Type	RADIUS Server
Server Name *	Enter Server Name
Server IP *	Enter Server IP
Authentication Port *	1812
<input type="checkbox"/> Enable Accounting	
Accounting Port	
Shared Secret *	Shared Secret
Group Name Attribute *	Enter Group Name Attribute

**Figure 129: Add RADIUS Server**

4. Click **Test Connection** to check the connectivity between the RADIUS server and Sophos XG Firewall. It also validates the RADIUS server user credentials.
5. Click **Save**.

#### Add TACACS+ Server

This page describes how to add a TACACS+ server.

1. Go to **Configure > Authentication > Servers** and click **Add**.
2. As **Server Type**, select **TACACS+ Server**.
3. Specify the TACACS+ server details:

#### Server Name

Specify a descriptive name for the TACACS+ server.

#### Server IPv4

Specify an IP address for the TACACS+ server.

#### Port

Specify the port of the TACACS+ server.

By default, this is port 49.

#### Shared Secret

Specify the shared secret which is a text string that serves as a password between a TACACS+ client and a TACACS+ server.

Server Type	<input type="text" value="TACACS+ Server"/>
Server Name *	<input type="text" value="Enter Server Name"/>
Server IPv4 *	<input type="text" value="Enter Server IPv4"/>
Port *	<input type="text" value="49"/>
Shared Secret *	<input type="text" value="Shared Secret"/>

**Figure 130: Add TACACS+ Server**

4. Click **Test Connection** to check the connectivity between the TACACS+ server and Sophos XG Firewall. It also validates the TACACS+ server user credentials.
5. Click **Save**.

### Add eDirectory Server

This page describes how to add an eDirectory server.

1. Go to **Configure > Authentication > Servers** and click **Add**.
2. As **Server Type**, select **eDirectory**.
3. Specify the eDirectory server details:

#### Server Name

Specify a descriptive name for the eDirectory server.

#### Server IP/Domain

Specify an IP address or domain for the eDirectory server.

#### Port

Specify the port of the eDirectory server.

By default, this is port 389.

#### Username

Specify a username for the eDirectory server.

#### Password

Specify a password for the eDirectory server.

#### Connection Security

Select the connection security for the eDirectory server:

- **Simple:** User credentials will be sent unencrypted as plaintext.
- **SSL:** Secure Sockets Layer. This is the most common method used for secured connection. The **Port** will then change from 389 (LDAPClosed) to 636 (ldaps = LDAP over SSL).
- **TLS:** Transport Layer Security. Same secure connection as SSL but uses the default port.

#### Base DN

Specify the Base DN for the eDirectory server. The Base DN is the starting point relative to the root of the eDirectory tree where the users are included who are to be authenticated. Note that the Base DN must be specified by the full distinguished name (DN) in LDAP notation, using commas as delimiters (e.g., O=Example,OU=RnD).

#### Get Base DN

Click **Get Base DN** if you are not aware about the Base DN. The Base DN is automatically retrieved from the directory.

Server Type	eDirectory
Server Name *	<input type="text"/>
Server IP/Domain *	<input type="text"/>
Port *	<input type="text"/> 389
Username *	<input type="text"/>
Password *	<input type="password"/>
Connection Security *	Simple
Base DN *	<input type="text"/>
<a href="#">Get Base DN</a>	

**Figure 131: Add eDirectory Server**

4. Click **Test Connection** to check the connectivity between the eDirectory server and Sophos XG Firewall. It also validates the eDirectory server user credentials.
5. Click **Save**.

## Services

This page allows you to configure authentication for firewall, VPN and admin traffic.

You can also configure global settings, NTLM settings, web client settings, Captive Portal parameters and Radius client settings for Single Sign-On server.



**Note:** You can also view and manage the authentication status on the **Monitor & Analyze > Diagnostics > Services** page.

Once you have deployed the device, the default access policy is automatically applied which will allow complete network traffic to pass through the device. This will allow you to monitor user activity in your network based on the default policy.

As device monitors and logs user activity based on the IP address, all the reports are also generated based on the IP address. To monitor and log user activities based on usernames or logon names, you have to configure the device for integrating user information and authentication process. Integration will identify access requests based on usernames and generate reports based on usernames.

When the user attempts to access, the device requests a user name and password and authenticates the user's credentials before giving access. User level authentication can be performed using the local user database on the device, external ADS server, LDAP, RADIUS or TACACS+ server.

To set up the user database

1. Integrate ADS, LDAP, RADIUS or TACACS+ if external authentication is required.
2. Configure for local authentication.
3. Register user

The device provides policy-based filtering that allows defining individual filtering plans for various users of your organization. You can assign individual policies to users, or a single policy to a number of users (group).

The device detects users as they log on to a Windows domain in your network via client machines. Users are allowed or denied access based on username and password. In order to authenticate a user, you must select at least one database against which the device should authenticate users.

To filter the Internet requests based on policies assigned, the device must be able to identify a user making a request.

You can configure Administrator, Firewall, VPN, and SSL VPN authentication through one or more servers.

This section covers the following topics:

## Firewall Authentication Methods

### Authentication Server List

Select an authentication server.

**Authentication Server List** displays all the configured servers while **Selected Authentication Server List** displays servers that will be used for authentication when the user tries to login.

In case of multiple servers, the authentication request is forwarded as per the order configured in the **Selected Authentication Server** list.

### Default Group

Select the default group for firewall authentication.

The screenshot shows the 'Authentication Server List' configuration screen. On the left, under 'Authentication Server List', there is a search bar labeled 'type to search...' and two checkboxes: 'Local' (which is checked) and 'Sophos'. On the right, under 'Selected Authentication Server', the 'Local' server is listed with a blue 'x' button to its right. A note 'drag to change priority' is displayed below the lists. At the bottom, there are buttons for 'Default Group' and 'Open Group'.

**Figure 132: Firewall Authentication Methods**

## VPN (IPsec/L2TP/PPTP) Authentication Methods

### Set Authentication Methods Same As Firewall

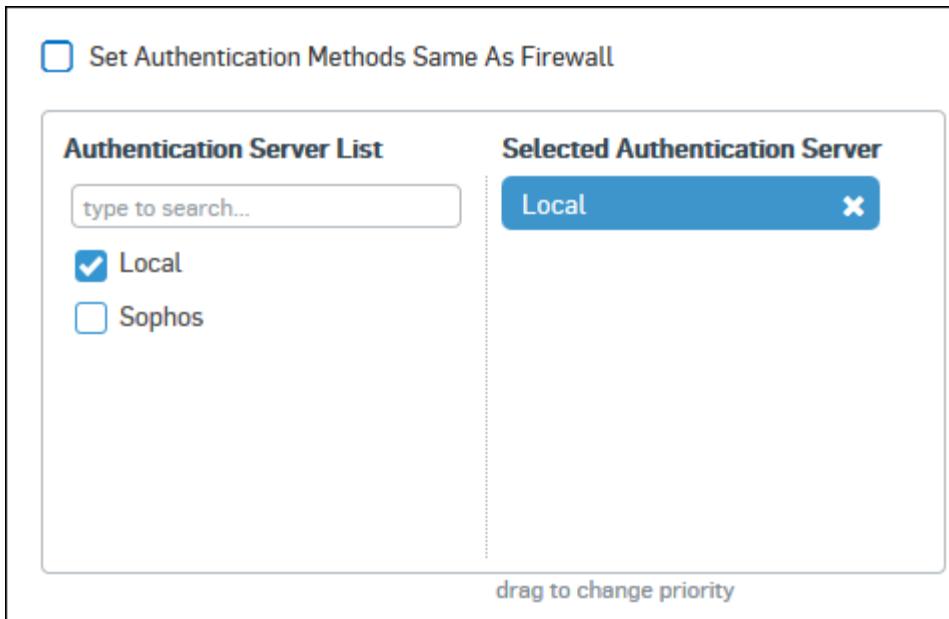
Enable to use the same authentication method as configured for the firewall traffic. If enabled all the authentication servers configured for the firewall traffic will be available for VPN traffic authentication configuration.

**Authentication Server List** displays all the configured servers while **Selected Authentication Server** list displays servers that will be used for authentication when user tries to login.

Override the authentication method for VPN traffic by selecting or deselecting any authentication server.

In case of multiple servers, the authentication request will be forwarded as per the order configured in the **Selected Authentication Server** list.

If RADIUS server authenticates users then PPTP and L2TP connections established using MSCHAPv2 or CHAP protocol can be authenticated through RADIUS.



**Figure 133: VPN (IPsec/L2TP/PPTP) Authentication Methods**

#### Administrator Authentication Methods

You can configure and manage authentication settings for all administrator users except for the super administrator.

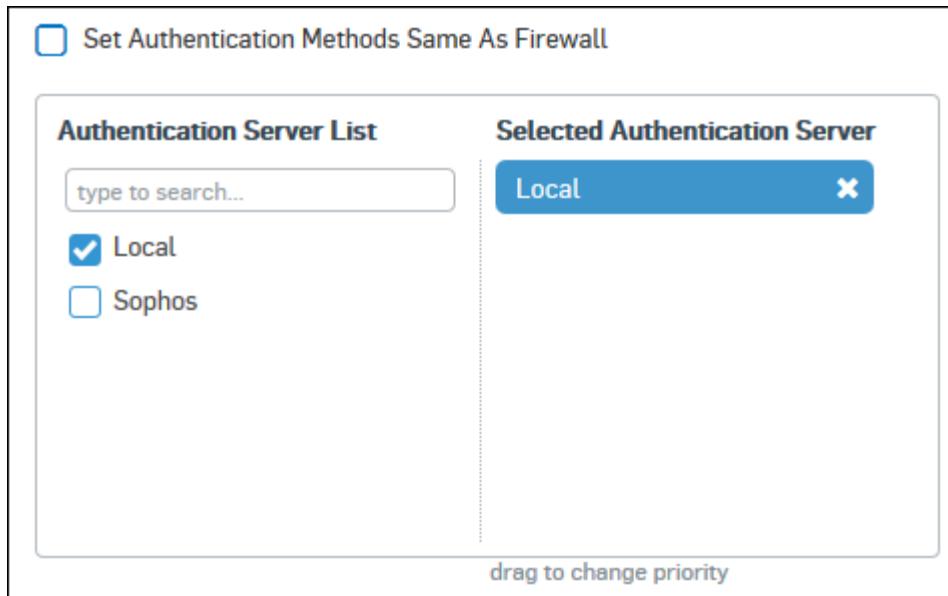
##### Set Authentication Methods Same As Firewall

Select to use the same authentication method as configured for firewall traffic. If enabled all the authentication servers configured for the firewall traffic will be available for administrator traffic authentication configuration.

**Authentication Server List** displays all the configured servers while **Selected Authentication Server** list displays servers that will be used for authentication when user tries to login.

Override the authentication method for administrator traffic by selecting or deselecting any authentication server.

In case of multiple servers, the authentication request will be forwarded as per the order configured in the **Selected Authentication Server** list.



**Figure 134: Administrator Authentication Methods**

### **SSL VPN Authentication Methods**

#### **Same as VPN**

Enable to use the same authentication method as configured for VPN traffic.

#### **Same as Firewall**

Enable to use the same authentication method as configured for the firewall traffic

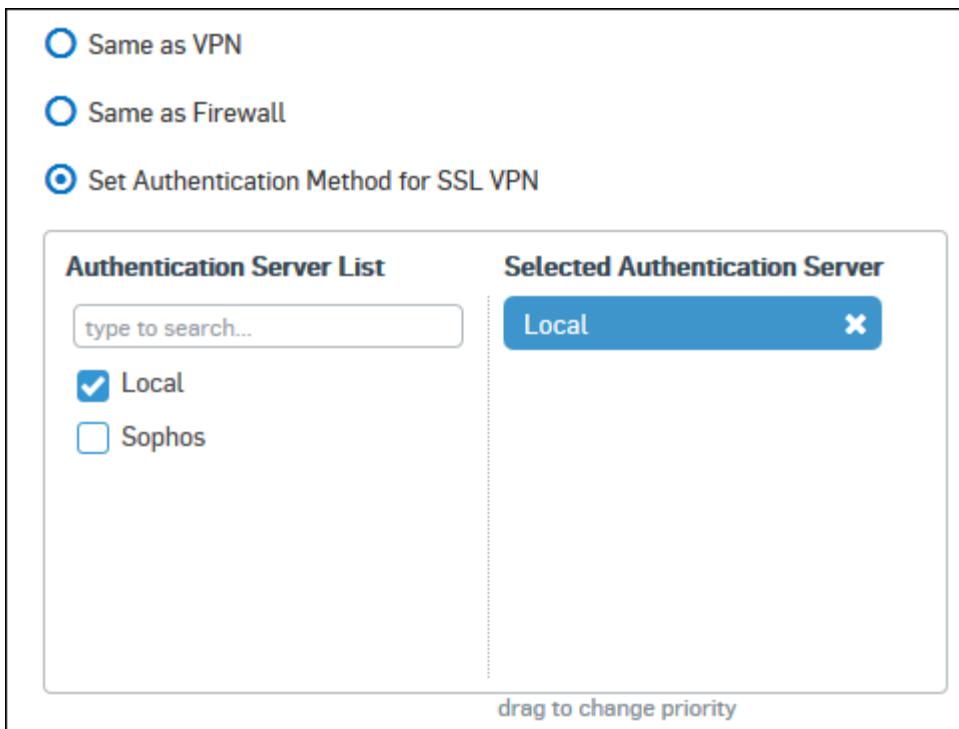
#### **Set Authentication Method for SSL VPN**

Enable to configure the authentication server for SSL VPN.

**Authentication Server List** displays all the configured servers while **Selected Authentication Server** list displays servers that will be used for authentication when user tries to login.

Override the authentication method for SSL VPN traffic by selecting or deselecting any authentication server.

In case of multiple servers, the authentication request will be forwarded as per the order configured in the **Selected Authentication Server** list.



**Figure 135: SSL VPN Authentication Methods**

### Global Settings

#### Maximum Session Timeout

Specify the timeout duration in minutes.

**Maximum Session Timeout** is the time in minutes a user is logged into the device. Exceeding the period, the user will be logged out automatically and the user must re-authenticate. This is applicable to administrative sessions only.

Acceptable range: 3 to 1440 minutes

Enable **Unlimited** to allow the users to remain logged in.

#### Simultaneous Logins

Specify the maximum number of concurrent logins allowed to the user.

Acceptable range: 1 to 99 concurrent logins

Alternatively, enable **Unlimited** to allow unlimited concurrent logins to the user.



**Note:** Login restriction is applicable only to those users who are added after this configuration.

Maximum Session Timeout * <input checked="" type="checkbox"/> Unlimited	<input type="text"/> Minutes (Between 3-1440)
Simultaneous Logins * <input type="checkbox"/> Unlimited	<input type="text"/> 1 (1-99)

**Figure 136: Global Settings**

### NTLM Settings

#### Inactivity Time

Specify the inactivity time in minutes.

The user inactivity timeout is the inactive/idle time in minutes after which the user will be logged out and has to re-authenticate.

Acceptable range: 6 to 1440 minutes

Default: 6 minutes

#### **Data Transfer Threshold**

Specify the minimum data to be transferred.

If the minimum data is not transferred within the specified time, the user will be marked as inactive.

Default: 1024 bytes

#### **HTTP challenge redirect on Intranet Zone**

Enabled: When a site hosted on the Internet initiates the NTLM web proxy challenge for authentication, the device redirects NTLM authentication challenge to the Intranet zone. The client is transparently authenticated through the device's local interface IP and credentials are exchanged only in the Intranet zone. User credentials remain protected.

Disabled: The client is transparently authenticated by the browser through the device by sending user credentials over the Internet.

Default: Enabled

Inactivity Time	6	Minutes (Between 6-1440)
Data Transfer Threshold	1024	Bytes
HTTP challenge redirect on Intranet Zone	<input checked="" type="checkbox"/> Enable	

**Figure 137: NTLM Settings**

#### **Web Client Settings (iOS and Android and API)**

##### **Inactivity Time**

Specify the inactivity time in minutes.

The user inactivity timeout is the inactive/idle time in minutes after which the user will be logged out and has to re-authenticate.

Acceptable range: 6 to 1440 minutes

Default: 6 minutes

##### **Data transfer threshold**

Specify the minimum data to be transferred.

If the minimum data is not transferred within the specified time, the user will be marked as inactive.

Default: 1024 bytes

Inactivity Time	6	Minutes (Between 6-1440)
Data Transfer Threshold	1024	Bytes

**Figure 138: Web Client Settings**

#### **SSO using RADIUS accounting request**

Device can authenticate users transparently who have already authenticated on an external RADIUS server.

## RADIUS Client IPv4

Specify the IPv4 address of the RADIUS client.

Only requests from the specified IP address will be considered for SSO.

### Shared Secret

Provide shared secret for authentication.

### Show Shared Secret

Click **Show** to view the configured shared secret.

Radius Client IPv4	Shared Secret	Show Shared Secret	Edit
<input type="text"/>	<input type="password"/>	Show	<input type="button" value="Edit"/> <input type="button" value="Delete"/>

**Figure 139: SSO using radius accounting request**

## Web Policy Actions for Unauthenticated Users (Captive Portal)

### Prompt unauthenticated users to login

Select **Yes** to redirect the access request of unauthenticated users either to the Captive Portal or Custom Message page.

Select **No** to drop unauthenticated user traffic. Unauthenticated users will not be redirected to the Captive Portal or the Custom Message page.

### Login prompt method

Configure where the unauthenticated user access requests should be redirected to.

Available Options:

- Include link to the Captive Portal in the User Notification message
- Display a custom message

Select **Include link to the Captive Portal in the User Notification message**, if an unauthenticated user access request is to be forwarded to the Captive Portal page.

#### Captive Portal uses HTTPS

If enabled, the user gets access to the Captive Portal page through secure channel.

Default: Enabled

#### Provide link to full User Portal

If enabled, the User Portal link is available on the Captive Portal page.

Default: Enabled

#### Redirect to a URL after login

If enabled, the user gets redirected to the user requested page or custom page.

#### URL to redirect

If request is to be redirected to the custom page, click **Custom URL** and specify the URL, else click **User requested URL**.

#### Preserve captive portal after login

Select **Yes** to minimize the Captive Portal popup, once the user is successfully authenticated.

Selecting **No** lets the Captive Portal to be displayed on system screen after successful authentication.

#### Use keep alive to maintain user session

Disable to logout the user after the configured inactivity time. If disabled, specify **User**

### Inactivity Timeout and Data Transfer Threshold.

The keep alive request is constantly exchanged between the device and user to check whether the user has logged out or is idle. If the device does not receive a response, the user is logged out automatically.

The more concurrent HTTP Captive Portal users there are, the more keep-alive requests are exchanged. In case of multiple concurrent HTTP Captive Portal users we recommend to disable this option.

Default: Enabled

- **User Inactivity Timeout**

User Inactivity timeout is the inactive/idle time in minutes after which user will be logged out and has to re-authenticate. Enable and specify timeout duration in minutes.

Acceptable range: 3 to 1440 minutes

Alternatively, select the checkbox **Unlimited** to keep the user logged in.

Default: Disabled

- **Data Transfer Threshold**

Specify a threshold value in bytes for the data transfer. If the minimum data is not transferred within the specified time, the user will be marked as inactive.

Select **Display a custom message**, if unauthenticated user is to be displayed custom message.

#### Page Header Image

Select **Default** to display the default image shipped with the device at the top of the custom message page, or select **Custom** to browse and upload a customized image.

Supported image format: JPG, PNG or GIF

Size: 700 X 80 pixels

#### Page Footer Image

Select **Default** to display the default image shipped with the device at the bottom of the custom message page, or select **Custom** to browse and upload a customized image.

Supported image format: JPG, PNG or GIF

Size: 700 X 80 pixels

#### Custom Message

Specify a message. You can customize the message to include the client IP address, category, and URL.

##### Blink Custom Message

Enable this option to display a blinking message.

##### Preview

Preview and check how the message will be displayed before saving the configuration.

Prompt unauthenticated users to login	<input type="radio"/> Yes <input checked="" type="radio"/> No (Display regular User Notification)
Login prompt method	<input checked="" type="radio"/> Include link to the Captive Portal in the User Notification message <input type="radio"/> Display a custom message
Captive Portal uses HTTPS	<input checked="" type="checkbox"/> Enable
Provide link to full User Portal	<input checked="" type="checkbox"/> Enable
Redirect to a URL after login	<input checked="" type="checkbox"/> Enable
URL to redirect	<input type="radio"/> User requested URL <input checked="" type="radio"/> Custom URL <input type="text" value="www.sophos.com"/>
Preserve captive portal after login	<input checked="" type="radio"/> Yes <input type="radio"/> No
Use keep alive to maintain user session	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
User inactivity timeout	<input checked="" type="checkbox"/> Unlimited <input type="text"/> Minutes (Between 3-1440)
Data transfer threshold	<input type="text"/> Bytes

**Figure 140: Captive Portal Settings**

## Groups

The Groups page displays a list of all the default and custom groups.

A group is a collection of users having common policies that can be managed as a single unit thus providing the possibility to assign various policies to a number of users in one operation/step. Users that belong to a particular group are referred to as group users.

A group can contain default as well as custom policies.

Various policies that can be grouped are:

- Surfing quota policy which specifies the duration of surfing time and the period of subscription
- Access time policy which specifies the time period during which the user will be allowed access
- Network traffic policy which specifies the time allocated to cyclic/non-cyclic network traffic
- Traffic shaping policy which specifies the bandwidth allocated for upload and download traffic
- Remote access policy which controls the access of remote clients
- Clientless policy which controls the access of clientless users

### Creating a New User Group

This page describes how to configure a user group.

Once the appropriate group is assigned, the user will automatically inherit all the policies added to the group.

1. Go to **Configure > Authentication > Groups** and click **Add**.
2. Specify the user group details.

#### Group Name

Enter a unique name for the group.

#### Description

Specify a description for the group.

#### Group Type

Select the group type.

#### Available Options:

- **Normal** - The user of this group needs to log on using the client device to access the Internet.

- **Clientless** - The user of this group does not need to log on using the client device to access the Internet and is symbolically represented by “group name (C)”. Access control is performed through the IP address.

The screenshot shows a configuration interface for a user group. At the top left is a label "Group Name \*". To its right is a text input field with the placeholder "Enter Group Name". Below this is a label "Description" followed by a larger text area labeled "Description". At the bottom left is a label "Group Type \*". To its right is a dropdown menu with the option "Normal" selected. There is also a small downward arrow icon next to the dropdown.

**Figure 141: User Group Details**

### 3. Specify the Policies.

#### Surfing Quota

Select the surfing quota policy from the list.



**Note:** For the group type **Clientless**, the option **Unlimited** is automatically applied.

#### Access Time

Select the access time policy from the list.



**Note:** For the group type **Clientless**, the option **Unlimited** is automatically applied.

#### Network Traffic (*not available for the Clientless group*)

Select the network traffic policy from the list.

Configured policy will be applicable to all the users who are member of this group.

#### Traffic Shaping

Select the traffic shaping policy from the list.

Configured policy will be applicable to all the users who are member of this group.

#### Remote Access

By default, the user will inherit his group's policy. To override the group policy, select a policy from the list.

You can also create a new policy directly on this page or from **VPN > SSL VPN (Remote Access) > VPN > SSL VPN (Remote Access)** page.

If a user shall not be provided SSL VPN access then select **No Policy Applied**.

#### Clientless

By default, the user will inherit his group's policy. To override the group policy, select the policy from the list.

You can also create a new policy directly on this page or from **VPN > Clientless Access > VPN > Clientless Access** page.

If a user shall not be provided SSL VPN access then select **No Policy Applied**.

#### Quarantine Digest

Configure quarantine digest.

Quarantine digest is an email containing a list of quarantined spam messages filtered by the device and held in the user quarantine area. If configured, the device will mail the digest on hourly, daily

or weekly basis to the user. Digest also provides a link to the User Portal from where the user can access and take an action on quarantined messages.

Available Options:

- **Enable** - The user will receive the quarantine digest at the configured frequency. This setting overrides the group setting.
- **Disable** - The user will not receive quarantine digest. This setting overrides the group setting.



**Note:** Quarantine digest is not applicable to Wi-Fi devices.

## MAC Binding

Enable to bind the user to a MAC address. By binding a user to a MAC address, you are mapping the user with a group of MAC addresses.

### L2TP (*not available for the Clientless group*)

Enable to grant group members access through an L2TP connection.

### PPTP (*not available for the Clientless group*)

Enable to grant group members access through an PPTP connection.

### Login Restriction (*not available for the Clientless group*)

Select the appropriate option to specify the login restriction for the group.

Available Options:

- **Any Node** - Select to allow a user to login from any of the nodes in the network.
- **Selected Nodes** - Select to restrict user login to the specified nodes. Specify an IP address. For an existing group, you can add further nodes, edit a node or remove a node.
- **Node Range** - Select to allow the user to login from a range of IP address. Specify the IP address range.

For the options **Selected Nodes** and **Node Range**, only IPv4 addresses are permitted.

Surfing Quota *	<input type="text" value="Surfing Quota"/>	
Access Time *	<input type="text" value="Access Time"/>	
Network Traffic	<input type="text" value="None"/>	
Traffic Shaping	<input type="text" value="None"/>	
Remote Access *	<input type="text" value="No Policy Applied"/>	
Clientless *	<input type="text" value="No Policy Applied"/>	
Quarantine Digest *	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
MAC Binding	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
L2TP *	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
PPTP *	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
Login Restriction*	<input checked="" type="radio"/> Any Node <input type="radio"/> Selected Nodes <input type="radio"/> Node Range	

**Figure 142: Policies**

4. Click Save.



**Note:** User configuration - MAC binding and policies is given precedence over the group configuration.

### Adding Users to the Existing Groups

This page describes how to add a user to an existing group.

1. Go to **Configure > Authentication > Groups**
2. Select the group to which you want to add the users by clicking the respective icon in the Manage column.
3. Click **Add Member(s)**.  
A pop-up window **Add Group Member** appears providing a list of all the users who can be added to the group along with some details. To search for a user filter the list based on the name and/or the current group.
4. Select the user you want to add to the group. You can select a single user or multiple users on the same page.
5. Click **Add** to confirm adding the member to the group.
6. Click **Save**.

The user is added to the group. You can check this by editing the group and clicking the **Show Group Members** button.

### Viewing List of Group Members

This page describes how to check a user's membership in a group.

1. Go to **Configure > Authentication > Groups**.
2. Select the group for which you want view the group members and click the edit icon in the Manage column.

**3. Click Show Group Member(s).**

A pop-up **Group Members** appears providing the list of all the users who are member of the selected group along with their usernames.

**4. Click Close to close the **Group Members** pop-up window.**

## Users

The Users page displays the list of all users added in the device.

Users are identified by an IP address or a username and are assigned to a user group. All the users in a group inherit the policies defined for that group.

### User Types

The device supports the following types of users:

- Normal
- Clientless
- Single Sign-On
- Thin Client user
- WWAN user

A **normal** user has to log in into the device which requires a client (client.exe) on the user machine, or the user can use a HTTP client component and all the policy-based restrictions are applied.

A **clientless** user does not require a client component (client.exe) on the user machine.

If **Single Sign-On** settings are configured, users are automatically logged to the device.

**Thin client** users do not need to have a client installed on the user machine.

**WWAN users** can log on via WLAN.

Use the given decision matrix below to choose which type of the user should be created.

**Table 2: Decision matrix for adding a user**

Feature	Normal User	Clientless User	Single Sign On User
User login required	Yes	No	No
Type of Group			
Normal	Yes	No	Yes
Clientless	No	Yes	No
Apply login restriction	Yes	Yes	Yes
Apply Surfing Quota policy	Yes	No	Yes
Apply Access Time policy	Yes	No	Yes
Apply Traffic Shaping policy	Yes	Yes	Yes
Apply Web Filter Policy	Yes	Yes	Yes
Apply Application Group policy	Yes	Yes	Yes
Apply Network Traffic policy	Yes	No	Yes

The page displays a list of all the available users along their user IDs, names and usernames, user types, profiles, group memberships, and their activity status.



**Note:** You can also view and manage live users on the **Monitor & Analyze > Current Activities > Monitor & Analyze > Current Activities > Live Users** page.

## Registering a New User

This page describes how to create a new user and quickly configure a related policy.

Once a user is registered successfully, the page provides two more options:

- **Reset User Accounting** - Click to reset Internet usage time and data transfer of the user.
- **View Usage** - Click to view the Internet usage and data transfer usage for that user.

1. Go to **Configure > Authentication > Users** and click **Add**.

2. Specify the user details.

### Username

Enter a unique username for the user.

### Name

Enter a name for the user.

### Description

Specify a description for the user.

### Password

Specify a password and re-enter the same password for confirmation.

The password is case-sensitive.

### User Type

Select the type of user from the available options.

Available options:

- User
- Administrator

### Profile (*available only if User Type selected is Administrator*)

Select the administrator profile. The administrator will get access to various Admin Console menus as per the configured profile.

You can create a new profile directly from this page or from the **System > Profiles > Device Access** page after clicking **Add**.

### Email

Enter a email address of the user.

Use comma to separate multiple email addresses.

Username *	<input type="text" value="Enter Username"/>
Name *	<input type="text" value="admin"/>
Description	<input type="text" value="Description"/>
Password *	<input type="password" value="*****"/> <input type="text" value="Confirm Password"/>
User Type *	<input checked="" type="radio"/> User <input type="radio"/> Administrator
Profile *	<input type="button" value="Profile"/>
Email *	<input type="text" value="Enter Email Address"/> Use a comma to separate multiple email addresses

**Figure 143: Add User**

3. Specify the **Policies** details.

#### Group

Select a group in which the user is to be added. User will inherit all the policies assigned to the group.

#### Surfing Quota

By default, the user will inherit its group policy. To override the group policy, select the policy from the list.

You can also create a new policy directly from this page or from the **Protect > Web > Surfing Quotas** page.

#### Access Time

By default, the user will inherit its group policy. To override the group policy, select the policy from the list.

You can also create a new policy directly from this page or from the **System > Profiles > Access Time** page.

#### Network Traffic

By default, the user will inherit its group policy. To override the group policy, select the policy from the list.

You can also create a new policy directly from this page or from the **System > Profiles > Network Traffic Quota** page.

#### Traffic Shaping

By default, user will inherit its group policy. To override the group policy, select the policy from the list.

You can also create a new policy directly from this page or from the **System > Profiles > Traffic Shaping** page.

Group *	Select Here
Surfing Quota *	Surfing Quota
Access Time *	Access Time
Network Traffic	None
Traffic Shaping	None

**Figure 144: Policies**

- Specify the SSL VPN Policy details.

#### Remote Access

By default, the user will inherit its group policy. To override the group policy, select a policy from the list.

You can also create a new policy directly from this page or from the **Configure > VPN > SSL VPN (Remote Access)** page.

If the user is not to be provided SSL VPN access then select **No Policy Applied**.

#### Clientless

By default, the user will inherit its group policy. To override the group policy, select a policy from the list.

You can also create a new policy directly from this page or from the **Configure > VPN > Clientless Access** page.

If the user is not to be provided clientless access then select **No Policy Applied**.

#### L2TP

By default, the user is provided remote access through L2TP. Disable if remote access is not to be provided to the user.

If enabled, provide the IP address (IPv4/IPv6) to be leased to the user for L2TP access.

#### PPTP

By default, the user is provided remote access through PPTP. Disable if remote access is not to be provided to the user.

If enabled, provide the IP address (IPv4/IPv6) to be leased to the user for PPTP access.

#### CISCO™ VPN Client

By default, the user is provided remote access through CISCO VPN client. Disable if remote access is not to be provided to the user.

If enabled, provide the IP address (IPv4/IPv6) to be leased to the user for CISCO VPN access.



**Note:** To use this feature, CISCO™ VPN client needs to be configured from the **Configure > VPN > Cisco VPN Client** page.

#### Quarantine Digest

Configure the quarantine digest.

Quarantine digest is an email containing a list of quarantined spam messages filtered by the device and held in the user quarantine area. If configured, the device will mail the digest to the user at the

configured frequency. Digest also provides a link to the User Portal from where the user can access and take an action on quarantined messages.

Available options:

- **Enable** - The user will receive the quarantine digest daily. This option overrides the group setting.
- **Disable** - User will not receive quarantine digests. This option overrides the group setting.

 **Note:** This feature is only available for non-wifi devices.

### Simultaneous Logins

Specify the number of concurrent logins that will be allowed for the user or click **Unlimited** for allowing unlimited concurrent logins.

Acceptable range: 1 to 99

Default: 1

 **Note:** The specified setting will override the global setting specified in the client preferences.

### MAC Binding

Enable/disable **MAC Binding**. By binding the user to a MAC address, you are mapping the user with a group of MAC addresses.

If enabled, specify MAC addresses for example 01:23:45:67:89:AB.

Once you enable MAC binding, the user will only be able to login through pre-specified machines.

Use a comma to separate multiple MAC addresses. For example 01:23:45:67:89:AB, 01:23:45:67:89:AC.

### Login Restrictions

Select the appropriate option to specify the login restriction for the user.

Available options:

- **Any Node** - User will be able to login from any of the nodes in the network.
- **User Group Node(s)** - User will be able to login only from the nodes assigned to his group.
- **Selected Nodes** (*only available for IPv4*) - User will be able to login from the specified nodes only.
- **Node Range** (*only available for IPv4*) - User will be able to login from any of the IP addresses from the configured range.

The screenshot shows the 'SSL VPN Policy' configuration page. It includes fields for 'Remote Access' (No Policy Applied), 'Clientless' (No Policy Applied), 'L2TP' (Enable selected), 'PPTP' (Enable selected), 'CISCO™ VPN Client' (Enable selected), 'Quarantine Digest' (Enable selected), 'Simultaneous Logins' (As Per Global checked, Unlimited checked, Range [1-99]), 'MAC Binding' (Enable selected), and a 'MAC address List' input field with a note about comma-separated values. At the bottom, there are radio buttons for 'Login Restriction': Any Node (selected), User Group node(s), Selected Nodes, and Node Range.

**Figure 145: SSL VPN Policy****5. Select Administrator Advanced Settings (available only if the user type is Administrator)****Schedule for Device Access**

Schedule the device access.

The administrator will be able to access the device only during the time configured in the schedule.

**Login Restriction for Device Access**

Select the appropriate option to specify the login restriction for the user.

Available options:

- Any Node** - Administrator will be able to login from any of the nodes in the network.
- Selected Nodes** - Administrator will only be able to login from the specified nodes.
- Node Range** - Administrator will be able to login from any of the IP addresses from the configured range.

**Reset User Accounting (available only when editing a user)**

Click to reset the Internet usage time and network traffic of the user.

**View Usage (available only when editing a user)**

Click to view the Internet usage and data transfer usage.



**Note:** User configuration is given precedence over group configuration.

The screenshot shows the 'Administrator Advanced Settings' configuration page. It includes a dropdown for 'Schedule for Device Access' set to 'All the Time' and radio buttons for 'Login Restriction for Device Access': Any Node (selected), Selected Nodes, and Node Range.

**Figure 146: Administrator Advanced Settings****6. Click Save.**

## Reset User Accounting

This option allows you to reset the Internet usage time and data transfer of the user.

1. Edit the user account of the user whose data accounting you want to reset by clicking the  icon in the Manage column.
2. Click **Reset User Accounting** and **OK** to confirm.



**Note:** You cannot reset user accounting for the live user.

## View Usage

This page describes how to view the Internet usage and data transfer usage of users.

1. Go to **Configure > Authentication > Users**.
2. Edit the user account of the user whose data usage you want to view by clicking the  icon in the Manage column.
3. Click **View Usage**.  
A pop-up window displays policy information such as time allotted, renewal of the surfing quota cycle, the data transfer cycle and the spent Internet usage time. In addition it provides facts on the network traffic.
4. Select the month for which you want to display the usage information.
5. Click **OK** to return to the parent page.

## Importing User Information

The **Import Users** page allows you to add new users by importing user details from the file.

Instead of creating users again in the device, if you already have users detail in a csv file, you can upload the csv file.

1. Go to **Configure > Authentication > Users** and click **Import** to import the csv file.
2. Browse to include the complete path for migrating user's information file.
3. Please consider the csv file format requirements:
  - Header (first) row should contain field names. Format of header row:
    - Compulsory field: username
    - Optional fields: password, name, group, email address
  - Fields can be configured in any order.
  - Subsequent rows should contain values corresponding to each field in the header row.
  - Number of fields in each row should be same as in the header row.
  - An error will be displayed if data is not provided for any field specified in the header.
  - Blank rows will be ignored.
  - If no password field is included in the header row then it will be set the same as the username.
  - If no group name is included in the header row, the administrator will not be able to configure a group at the time of migration.
4. Click **Upload** to import the file.

## Exporting Users

This menu allows you to export user information.

1. Go to **Configure > Authentication > Users** and click **Export** to export the user details in a csv file.  
A pop-up window appears displaying the name of the csv file you are going to export.
2. Select to open or save the file.
3. Click **OK**.

The csv file is generated with the following headers: Name, Username, Enc\_password, Email Address, and Group.



**Note:** Backend users, that means users who are authenticated against a backend authentication service like Active Directory, will not be exported.

## Purging Active Directory Users

This page allows you to purge AD Users.

1. Go to **Configure > Authentication > Users** and click **Purge AD Users** to synchronize the device's Active Directory users with an external Active Directory server.

 **Note:** The purge operation will not interrupt user login/logout and accounting events. If HA is configured, user details are deleted from both, the primary device and the auxiliary device.

2. Click **OK** to confirm the message.

## Change Status

1. Go to **Configure > Authentication > Users**.
2. Select a user whose status is to be changed and click **Change Status** to change the status of that user. If the current status is **Enabled**, the status of the user will change to **Disabled** when you click this button and vice-versa.

## One-Time Password

On this page, you can configure the one-time password (OTP) service, and you can monitor or edit the tokens of the one-time-password users.

One-time passwords are a method to improve security for password-based authentication. The user-specific password, which is sometimes too weak, will be amended with a one-time password that is valid for only one login. Thus, even if an attacker gets hold of it, he will not be able to log in with it.

One-time passwords generally change consistently, in regular intervals, being calculated automatically by a specific algorithm. Soon after a new password is calculated, the old password expires automatically. To calculate one-time passwords, the user needs to have either a mobile device with an appropriate software, or a special hardware or security token. Hardware tokens are ready to use from the start. On the mobile device, the end user needs to install Sophos Authenticator or a similar software and deploy the configuration, which is available in the User Portal as a QR code, on the start page or on the OTP Token page (see User Portal page). Having done that, the device calculates one-time passwords in token-specific intervals. It is important that date and time are correct on the mobile device as the time stamp is used for one-time password generation.

 **Note:** To authenticate on the facilities where the one-time password is required, the user has to enter his user-specific device password, directly followed by the one-time password.

The administrator can also generate one-time passwords, also known as passcodes, manually. In this case, you have to ensure that these not time-limited one-time passwords are safely transmitted to the end user. This process, however, should only be considered as a temporary solution, for example when a user temporarily has no access to his or her password calculating device.

The page displays all existing one-time passwords. You can add, update or delete an OTP. For each OTP, the list shows:

### Username

Displays the user name of the OTP owner.

### Status

Displays the status of the OTP.

### Secret

Displays the 32-hex secret of the OTP.

### Related information

[Create OTP Token Automatically for Two-Factor Authentication](#)

### Add OTP Token

This page enables you to add and edit one-time password tokens.

1. Go to **Configure > Authentication > One-Time Password** and click the **Add** button.
2. Specify the following details for adding an OTP token:

#### Secret

This is the shared secret of the user's hardware token or soft token. A hardware token has an unchangeable secret, given by the hardware producer. The soft token is created randomly by Sophos XG Firewall, when **Auto-create OTP tokens for users** is enabled. The secret should have a hexadecimal format and consist of at least 32 characters.

#### User (optional)

Select the user to whom the token should be assigned.

#### Description (optional)

Add a description or other information. This text will be displayed for the administrator with the QR code. If you define different tokens for one person, e.g., a hardware token and a soft token for the mobile phone, it is useful to enter some explanation here as the user will be displayed all QR codes side by side.

#### Use custom token timestep

If you need another timestep for a token than the default token timestep defined in the OTP Settings section, enable this toggle switch and enter the value. The timestep defined here has to correspond with the timestep of the user's password generation device, otherwise authentication fails.

#### Timestep

Enter the value for the additional timestep.

Acceptable range: 10 - 300 seconds.

#### Additional Codes (Available only when editing OTP token)

You can add one-time passwords manually for a token. Click the Plus icon to generate the one-time passwords (10 at maximum). These one-time passwords are not time-limited. A one-time password will be deleted automatically when the user logged in with it.

Secret *	<input type="text" value="Enter Secret"/> <span style="color: red;">×</span>
User	<input type="text" value="None"/>
Description	<input type="text"/>
Use custom token timestep	<input checked="" type="checkbox"/> ON
Timestep	<input type="text" value="Enter Timestep in Seconds"/> <span style="float: right;">Seconds [10 - 300]</span>

**Figure 147: Add OTP Token**

3. Click **Save**.

The OTP token for the specific user has been created and appears in the one-time password list on the **One-time Password** page.

### Configure One-time Password

This page allows you to enable and configure the one-time password service.

1. Go to **Configure > Authentication > One-Time Password** and click the **Settings** button.

2. Activate the one-time password service by clicking on the **ON/OFF** slider.
3. Specify the OTP service status.

#### **OTP for all users**

If enabled, all users have to use one-time passwords. If only specific users should use one-time passwords, disable this option and select or add users or groups from the list.

#### **Auto-Create OTP Tokens for users**

If enabled, a QR code for configuring the mobile device software will be presented to the authorized users the next time they log in to the User Portal. For this to work, make sure that the users have access to the User Portal. When a user logs in to the User Portal, the respective token will appear in the OTP Tokens list. Enabling this feature is recommended when you are using soft tokens on mobile devices. If your users only use hardware tokens you should instead disable this option and add the tokens before enabling the OTP feature.

#### **Enable OTP for facilities**

Here, you select the Sophos XG Firewall facilities that should be accessed with one-time passwords by the selected users. When you select the **Auto-create OTP tokens for users** option, the User Portal needs to be enabled for security reasons: As the User Portal gives access to the OTP tokens, it should have no weaker protection itself.



**Note:** When selecting **WebAdmin** you have to ensure that the selected users have access to the one-time password tokens. Otherwise you may log them out permanently.

4. Specify the timestep settings.

#### **Default token timestep in seconds**

To synchronize one-time password generation on the mobile device and on the Sophos XG Firewall, the timestep has to be identical on both sides. Some hardware tokens use 60 seconds. Other software OTP tokens use a timestep of 30 seconds which is the default value here. If the timestep does not match, authentication fails.

Acceptable Range: 10 - 300 seconds

Default: 30 seconds

#### **Maximum passcode offset steps**

With help of this option you can set the maximum passcode offset steps. This means if you for example set 3 steps you restrict the clock of a token to drift no more than 3 timesteps between two logins.

Acceptable range: 0 - 10 steps

Default: 1 step

#### **Maximum initial passcode offset steps**

With help of this option you can set the maximum initial passcode offset steps. This means if you for example set 10 steps you restrict the clock of a token to drift no more than 10 timesteps between two logins. This option is only applied when the user employs the token for the very first time.

Acceptable range: 0 - 600 steps

Default range: 10 steps

The screenshot shows the 'One-Time Password' configuration page. At the top, there is a toggle switch labeled 'OFF' for 'One-Time Password'. Below it, the 'One-time password service status' section contains two toggle switches: 'OTP for all users' (ON) and 'Auto-create OTP tokens for users' (ON). Underneath these, the 'Enable OTP for facilities:' section lists several options with checkboxes: 'WebAdmin' (unchecked), 'SSL VPN Remote Access' (unchecked), 'User Portal' (unchecked), and 'IPsec Remote Access' (unchecked). Further down, the 'Timestep' section includes fields for 'Default token timestep in seconds' (set to 30), 'Seconds [10 - 300]', 'Maximum passcode offset steps' (set to 1), and '[0 - 10]', and 'Maximum initial passcode offset steps' (set to 10), with a range of '[0 - 600]'. The entire configuration is contained within a light gray bordered box.

**Figure 148: Configure OTP**

5. Click **Apply**.

## Captive Portal

The Captive Portal allows customization of the Captive Portal login page.

The device provides flexibility to customize the Captive Portal login page. This page can include your organization name and logo.

The device also supports a customized page in languages other than English.

External users, who need to use authentication services, are required to log in over the Captive Portal once before they get access to the User Portal. External users can access the Captive Portal by browsing to <https://<Sophos Device IP Address>:8090>. After login, external users have access to the User Portal and are listed on the **Configure > Authentication > Users** page. External users can access the User Portal by browsing to <https://<Sophos Device IP Address>> or clicking **Click here for User My Account** on the **Captive Portal** page.

1. Go to **Configure > Authentication > Captive Portal**.
2. Specify the **General Settings**.

### Logo

Decide which logo to use.

- **Custom** - Select to upload the custom logo and specify an image file name to be uploaded. Click **Browse** to browse and select the complete path.
- **Default** - Select to use the default logo

The image size should not exceed 125x70 pixels.

**Logo URL**

Provide an URL to be redirected to on clicking the logo.

Default: [/www.sophos.com](http://www.sophos.com)

**Page Title**

Change the page title if required.

Default: Network Authentication

**Login Page Header**

Provide the text to be displayed on the Captive Portal login page.

**Login Page Footer**

Provide a message to be displayed in the footer of the Captive Portal login page.

**Username Caption**

Provide a label for the textbox to be displayed on the Captive Portal login page.

Default: **Username**

**Password Caption**

Provide a label for the textbox to be displayed on the Captive Portal login page.

Default: **Password**

**Login Button Caption**

Provide a label for the button to be displayed on the Captive Portal login page.

Default: **Login**

**Logout Button Caption**

Provide a label for the button to be displayed on the Captive Portal login page.

Default: **Logout**

**User Portal Link Caption**

Provide a text to be displayed for the User Portal login page link. By clicking the link, the user will be directed to the User Portal login page.

Default: **Click here for User Portal**

Logo	<input checked="" type="radio"/> Default <input type="radio"/> Custom <input type="button" value="Browse..."/> No file selected.	Size 125x70 pixels
Logo URL *	www.sophos.com	
Page Title *	Network Authentication	
Login Page Header	<input type="text"/>	
	HTML Input	
Login Page Footer	<input type="text"/>	
	HTML Input	
Username Caption *	Username <input type="text"/>	
HTML Input		
Password Caption *	Password <input type="text"/>	
HTML Input		
Login Button Caption *	Login <input type="text"/>	
Logout Button Caption *	Logout <input type="text"/>	
User Portal Link Caption *	Click here for User Portal <input type="text"/>	

**Figure 149: General Settings****3. Specify the Color Scheme settings.**

Customize the color scheme of the Captive portal if required. Specify the color code or click the square box to pick the color.

Background Color	<input type="text" value="FFFFFF"/>	<input type="color"/>	Header, Footer Font Color	<input type="text" value="565656"/>	<input type="color"/>
Page Title Background Color	<input type="text" value="FFFFFF"/>	<input type="color"/>	Page Title Font Color	<input type="text" value="336699"/>	<input type="color"/>
Caption Font Color	<input type="text" value="565656"/>	<input type="color"/>			

**Figure 150: Color Scheme****4. Specify the Custom HTML Template settings.****Use Custom HTML Template**

Select to fully customize Captive Portal using custom HTML code.

**HTML Text**

Provide HTML code to render the Captive Portal according to your requirement. Dynamic contents like banners from external web servers, a customizable **Message of the day** box and so on can be integrated in the HTML code.

By default, sample HTML will be displayed.



**Note:** It is compulsory to have one HTML div element with ID \_\_loginbox (e.g. <div id='\_\_loginbox'>)The system will render necessary input elements in this div.



**Figure 151: Custom HTML Template**

5. Select from the following possibilities:

#### Apply

Click to save your settings.

#### Preview

Click to view the custom settings before saving the changes.

#### Reset To Default

Click to revert to the default settings.

## Guest Users

The Guest Users page displays a list of all the guest users added.

Users without a pre-existing user account who want to access the Internet using a hotspot, via a network available at the airport, hotels, hostels, etc., are called “guest users”. These users, that are otherwise considered unauthenticated and/or are denied access, are allowed to make a request to connect to the Internet for a limited time by authenticating themselves. Being authenticated, these users are authorized to access the Internet as guest user. At such public places, Internet access is secured by configuring access policies to restrict any malicious use of the network.

Sophos XG Firewall allows the administrator to pre-configure individual or multiple guest users using the Admin Console. The credentials of guest users configured via the Admin Console can be printed and handed over to the guest user. Alternately, guest users can register themselves using the guest user portal. The credentials and Internet access details of guest users registered via the guest user portal can either be sent via SMS or can be printed.

In case of successful authentication the guest user is granted access according to the applicable group, or else is redirected to the **Captive Portal** page.

You can filter the list based on the name or username of the user, cell phone number of the user, and validity of the user account, . The page also provides options to add a single or multiple users, distributing credentials for the Internet access, update user parameters, view or reset the data transfer usage.

Resend Credential – Click the Resend Credential icon  in the Manage column against a user registered via the Guest User Portal to whom the access detail's SMS are to be resent.

### Registering a Single Guest User

This page describes how to register a new single guest user.

This page allows you to manually enter and configure guest user details. Before adding a guest user, you have to configure the general settings on the **Configure > Authentication > Guest User Settings** page.

1. Go to **Configure > Authentication > Guest Users** and click **Add Single**.
2. Specify guest user details.

#### Username

Displays auto-generated username.

**Password**

Displays auto-generated password.

**Name**

Specify the name of the guest user.

**Email**

Specify the email address of the guest user.

**User Validity (Duration in Days)**

Specify the validity for the specified guest user in days.

Minimum number of days: 1 day

Maximum number of days: 999 days

**Validity Start**

Select the type from when a user's validity should be counted.

Available Options:

- **Immediately** - Validity is counted from the time the guest user is created.
- **After First Login** - Validity is counted from the time the guest user logs into the network for the first time.

<b>Username</b>	Auto-Generated
<b>Password</b>	Auto-Generated
<b>Name *</b>	<input type="text" value="Enter Name"/>
<b>Email *</b>	<input type="text" value="Email"/>
<b>User Validity (Duration in Days) *</b>	<input type="text"/>
<b>Validity Start *</b>	<input checked="" type="radio"/> Immediately <input type="radio"/> After First Login

**Figure 152: Add Guest User**

3. Click **Add** to register the guest user or **Add and Print** to register the user and print the login credentials.

**Reset User Accounting**

This option allows you to reset the Internet usage time and data transfer of the user.

1. Edit the user account of the user whose data accounting you want to reset by clicking the  icon in the Manage column.
2. Click **Reset User Accounting** and **OK** to confirm.

 **Note:** You cannot reset user accounting for the live user.

**View Usage**

This page describes how to view the Internet usage and data transfer usage of users.

1. Go to **Configure > Authentication > Users**.
2. Edit the user account of the user whose data usage you want to view by clicking the  icon in the Manage column.
3. Click **View Usage**.  
A pop-up window displays policy information such as time allotted, renewal of the surfing quota cycle, the data transfer cycle and the spent Internet usage time. In addition it provides facts on the network traffic.

4. Select the month for which you want to display the usage information.
5. Click **OK** to return to the parent page.

### Register Multiple Guest Users

This page describes how to create multiple guest users.

1. Go to **Configure > Authentication > Guest Users** and click **Add Multiple**.
2. Specify the guest user details.

#### Number of Users

Specify the number of guest users to be created.

#### User Validity (Duration in Days)

Specify the validity of multiple guest users in days.

Minimum number of day: 1 day

Maximum number of days: 999 days

#### Validity Start

Select the type from when the users' validity should be counted.

Available Options:**Immediately** - Validity is counted from the time the guest users are created.**After**

**First Login** - Validity is counted from the time one of the guest users just created logs into the network for the first time.

Number of Users *	<input type="text"/>
User Validity [Duration in Days] *	<input type="text"/>
Validity Start *	<input checked="" type="radio"/> Immediately <input type="radio"/> After First Login

**Figure 153: Add Guest User**

3. Click **Add** to register the users or **Add and Print** to register the users and print the login credentials.

The guest users have been created and appear on the **Guest Users** page.

 **Note:** The users only appear with the name “guest-XXX”. To allocate names to these entries, you have to edit each user.

### Update Guest User Configuration

This page describes how to change the policies configured for the guest user.

1. Go to **Configure > Authentication > Guest Users**.
2. Select the guest user for which you want to change the policies by clicking the  icon in the Manage column.
3. Update the guest user details.

#### Username

Displays the username of the guest user.

#### Name

Change the name of the guest user if required.

#### Description

Specify a description of the guest user.

#### Password

Displays the password in encrypted format.

You can change the password by clicking on **Change Password**.

If you change it, enter the new password in the **Password** field and re-enter it in the **Confirm Password** field.

#### Cell Phone Number

Displays the cell phone number.



**Note:** The cell phone number cannot be edited.

#### Email

Change the the email address of the guest user if required.

#### Internet Usage Time

Displays total Internet usage time information in HH:MM format.

Username *	guest-00002
Name *	guest-00002
Description	Description
Password *	***** <a href="#">Change Password</a>
Cell Phone Number *	
Email *	Enter Email Address
Internet Usage Time	00:00 (HH:MM)

Use a comma to separate multiple email addresses

**Figure 154: Edit Guest User**

#### 4. Specify the Policies.

##### Group

Displays the group to which the user belongs. User will inherit all the policies assigned to the group.



**Note:** The guest user group cannot be edited.

##### Surfing Quota

Select the surfing quota policy from the list.

You can also create a new policy directly from this page by selecting **Create new** and attach it to the user.

##### Access Time

Select the access time policy from the list.

You can also create a new policy directly from this page by selecting **Create new** and attach it to the user.

##### Network Traffic

Select the network traffic policy from the list.

You can also create a new policy directly from this page by selecting **Create new** and attach it to the user.

##### Traffic Shaping

Select the traffic shaping policy from the list.

You can also create a new policy directly from this page by selecting **Create new** and attach it to the user.

 **Note:** User configuration is given precedence over group configuration i.e. user MAC binding and policies configuration is given priority over group configuration.

Group *	Guest Group
Surfing Quota *	Unlimited Internet Access
Access Time *	Allowed all the time
Network Traffic	None
Traffic Shaping	None

**Figure 155: Policy**

- Specify the SSL VPN Policy details.

#### Remote Access

Select a policy for remote access from the list or create a new one. To create a new policy, select **Create new**.

You can create a new policy directly from this page or from the **Configure > VPN > SSL VPN (Remote Access)** page.

#### Clientless

Select a policy for clientless access from the list or create a new one. To create a new policy, select **Create new**.

You can create a new policy directly from this page or from the **Configure > VPN > Clientless Access** page.

If a user is not to be provided SSL VPN access then select **No Policy Applied**.

#### L2TP

Enable if you are mapping the user to get access through L2TP connection.

Provide the IP address to be leased to the guest user for L2TP access.

#### PPTP

Enable if you want to allow the user to get access through a PPTP connection.

If enabled, provide the IP address (IPv4/IPv6) to be leased to the guest user for PPTP access.

#### CISCO™ VPN Client

By default, the user is provided remote access through the CISCO VPN client. Disable if remote access is not to be provided to the user.

If enabled, provide the IP address (IPv4/IPv6) to be leased to the user for CISCO VPN access.

 **Note:** To use this feature, CISCO™ VPN client needs to be configured from the **Configure > VPN > Cisco VPN Client** page.

#### Quarantine Digest

Configure the quarantine digest.

Quarantine digest is an email and contains a list of quarantined spam messages filtered by the device and held in the user quarantine area. If configured, the device will mail the quarantine digest to the user every day. The digest provides a link to the user's **My Account** from where the user can access his quarantined messages and take the required action.

Available Options:

- **Enable** - User receives the quarantine digest daily. This option overrides the group setting.
- **Disable** - User does not receive quarantine digests. This option overrides the group setting.



**Note:** Quarantine digest is not applicable to Wi-Fi devices.

### Simultaneous Logins

Specify the number of concurrent logins that will be allowed to the user or click **Unlimited** for allowing unlimited concurrent logins.

The specified setting overrides the global setting specified in the client preferences.

### MAC Binding

Enable/disable **MAC Binding**. By binding the user to a MAC address, you are mapping the user with a group of MAC addresses.

For **Selected Nodes** and **Node Range** only IPv4 addresses can be provided.

### MAC address List

Specify MAC addresses, for example 01:23:45:67:89:AB.

Once you enable MAC binding, the user can login through pre-specified machines only.

To configure multiple MAC addresses use commas. For example 01:23:45:67:89:AB, 01:23:45:67:89:AC.

### Login Restriction

Select the appropriate option to specify the login restriction for the user.

Available Options:

- **Any Node** - User can login from any of the nodes in the network.
- **User Group Node(s)** - User can login only from the nodes assigned to the group.
- **Selected Nodes** - User can login from the specified nodes only.
- **Node Range** - User can login from any of the IP addresses from the configured range.

The screenshot shows the configuration interface for an SSL VPN policy. It includes fields for Remote Access (No Policy Applied), Clientless (No Policy Applied), L2TP (Enable selected), PPTP (Enable selected), CISCO™ VPN Client (Enable selected), Quarantine Digest (Disable selected), Simultaneous Logins (As Per Global checked, Unlimited checked, 1 selected), MAC Binding (Enable selected), and a MAC address List input field. At the bottom, there are options for Login Restriction: Any Node (selected), User Group node(s), Selected Nodes, and Node Range.

Setting	Value
Remote Access *	No Policy Applied
Clientless *	No Policy Applied
L2TP *	<input type="radio"/> Enable <input checked="" type="radio"/> Disable IP Address [ ]
PPTP *	<input type="radio"/> Enable <input checked="" type="radio"/> Disable IP Address [ ]
CISCO™ VPN Client *	<input type="radio"/> Enable <input checked="" type="radio"/> Disable IP Address [ ]
Quarantine Digest *	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Simultaneous Logins *	<input checked="" type="checkbox"/> As Per Global <input type="checkbox"/> Unlimited [1] [1-99]
MAC Binding *	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
MAC address List	Use a comma or a new line to separate multiple MAC addresses. Example: 11:11:11:11:11:11, 22:22:22:22:22:22
Login Restriction*	<input checked="" type="radio"/> Any Node <input type="radio"/> User Group node(s) <input type="radio"/> Selected Nodes <input type="radio"/> Node Range

Figure 156: SSL VPN Policy



**Note:** Before saving, you have two more options on this page

- **Reset User Accounting** - Click to restart the accounting of the guest user's Internet usage.
- **Note:** You cannot reset the user accounting of live users.
- **View Usage** - Click to view the Internet usage information of a particular guest user.

## 6. Click Save .

The guest user settings have been updated.

## Clientless Users

The Clientless Users page displays a list of all the clientless users.

Clientless users are the users who can bypass the client login to access the Internet and are managed by the device itself. As clientless users can bypass the device login, create clientless users when your network has few Non-Windows machines, VOIP boxes, or servers.

### Add a Single Clientless User

This page describes how to add a single clientless user.

1. Go to System > Authentication > Clientless Users and click Add.
2. Specify the clientless users details.

#### Username

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

#### IP Address

Specify an IP address(IPv4/IPv6) for the clientless user.

#### Group

Select a group to which the user is to be added. The user will inherit all the policies assigned to the group.

Change the policies applied to the user by editing the user details (once the user has been created).

#### Name

Enter a unique name for the user.

#### Email

Specify an email address.

#### Quarantine Digest

Configure quarantine digest. Quarantine digest is an email and contains a list of quarantined spam messages filtered by the device and held in the user quarantine area. If configured, the device will mail the quarantine digest to the user every day. The digest provides a link to the User Portal from where the user can access quarantined messages and take the required action.

Available Options:

- **Enable** - User will receive the quarantine digest daily. This option overrides the group setting.
- **Disable** - User will not receive quarantine digests. This option overrides the group setting.
- **Apply Group Settings** - User will receive quarantine digests as configured for the group the user belongs to.

**Note:** Quarantine digest is not available for Wi-Fi devices.

#### Description

Specify a user description.

**Figure 157: Add Clientless User**

By clicking the icon you can add further users.

By clicking the icon you can remove users.

3. Click **Save**.

### Reset User Accounting

This option allows you to reset the Internet usage time and data transfer of the user.

1. Edit the user account of the user whose data accounting you want to reset by clicking the icon in the Manage column.
2. Click **Reset User Accounting** and **OK** to confirm.

**Note:** You cannot reset user accounting for the live user.

### View Usage

This page describes how to view the Internet usage and data transfer usage of users.

1. Go to **Configure > Authentication > Users**.
2. Edit the user account of the user whose data usage you want to view by clicking the icon in the Manage column.
3. Click **View Usage**.  
A pop-up window displays policy information such as time allotted, renewal of the surfing quota cycle, the data transfer cycle and the spent Internet usage time. In addition it provides facts on the network traffic.
4. Select the month for which you want to display the usage information.
5. Click **OK** to return to the parent page.

### Add Multiple Clientless Users

This page describes how to add multiple clientless users.

1. Go to **Configure > Authentication > Clientless Users** and click **Add Range**.
2. Specify the following:

#### From IP

Specify a Start-IP address for the range.

#### To IP

Specify an End-IP address for the range.

#### Group

You can change the policies applied to the user by editing the user details. If you change the policies for the user, user specific policies will take precedence over user group policies.

From IP *	<input type="text" value="Enter IP Address"/>
To IP *	<input type="text" value="Enter IP Address"/>
Group *	<input type="text" value="Clientless Open Group"/>

**Figure 158: Clientless User**

3. Click **Save**.

The users have been created and appear on the **Clientless Users** page.

 **Note:** The users only appear with their IP addresses. To allocate names to these addresses, you have to edit each user.

### Changing Policies of the Clientless User

This page describes how to change the policies configured for a clientless user.

Changing the policies applied to a user can be performed by updating the user details. If you change the policies for the user, user specific policies will take precedence over user group policies.

1. Go to **Configure > Authentication > Clientless Users**.
2. Select the user for which you want to change the policies by clicking the  icon in the Manage column.
3. Update the **Policies**.

#### Traffic Shaping

Change the Traffic Shaping policy applied to the user.

The policy applied here will take the precedence over the group policy.

You can also create a new traffic shaping policy on this page or on the **System > Profiles > Traffic Shaping** page.

#### Quarantine Digest

Configure quarantine digest.

Quarantine digest is an email and contains a list of quarantined spam messages filtered by the device and held in the user quarantine area. If configured, the device will mail the quarantine digest every day to the user. The digest provides a link to the **User Portal** from where the user can access his quarantined messages and take the required action.

#### Available Options:

- **Enable** - User will receive the quarantine digest daily. This option overrides the group setting.
- **Disable** - User will not receive quarantine digests. This option overrides the group setting.

 **Note:** Quarantine digest is not available for Wi-Fi devices.

Traffic Shaping	<input type="text" value="None"/>
Quarantine Digest *	<input checked="" type="radio"/> Enable <input type="radio"/> Disable

**Figure 159: Policies**

 **Note:** Before saving, you have two more options on this page.

- **Reset User Accounting** - Click to reset the Internet usage time and data transfer of the user.



**Note:** You cannot reset the user accounting of live users.

- [View Usage](#) - Click to view the Internet usage and data transfer usage.

#### 4. Click Save.

## Guest User Settings

This page allows you to configure general settings, registration settings and SMS gateway for guest users.

Users without a pre-existing user account wanting to access the Internet using a hotspot, or via a network available at the airport, hotels, hostels, etc. are called “guest users”. These users, that are otherwise considered unauthenticated and/or denied access, are allowed to make request to connect to the Internet for a limited period by authenticating themselves. On being authenticated, these users are authorized to access Internet as guest users. At such locations, Internet access is secured by configuring access policies to restrict any malicious use of the network.

Sophos XG Firewall allows administrator to pre-configure single or multiple guest users using the Admin Console. The credentials of guest users configured via the Admin Console can be printed and handed over to the guest user. Alternately, guest users can register themselves using the guest user portal. The credentials and Internet access details of guest users registered via the guest user portal can either be sent via SMS or can be printed.

In case of successful authentication the guest user is granted access according to the applicable group, or else is redirected to the **Captive Portal** page.

The page allows configuring general parameters to provide secured Internet access for guest users.

1. Go to **Configure > Authentication > Guest User Settings**.
2. Specify the **Guest User General Settings**.

### Username Prefix

Enter a prefix to be used for auto-generation of a username for guest users.

Default: guest

### Group

Select a group of policies to assign to guest users or create a new one.

**Note:** You can create a new group of policies directly from this page or from the **Configure > Authentication > Groups** page.

### Password Length

Specify the length of the auto-generated password for Guest Users.

Acceptable range: 3 to 60 characters

Default: 8 characters

The password length is a basic security parameter, the value of which affects the strength of password against brute force attack.

### Password Complexity

Select a type of password from the available options to be used for complexity of an auto-generated password:

Available options:

- **Numeric Password** – Password will include only numeric characters.
- **Alphabetic Password** – Password will include only alphabetic characters.
- **Alphanumeric Password** – Password will include numeric as well as alphabetic characters.
- **Alphanumeric with Special Character Password** - Password will include numeric, alphabets and special characters.

The password strength is a function of its length, complexity, and unpredictability. Combining password length with password complexity makes a password difficult to guess.

## Disclaimer

Provide the disclaimer message to be printed below every user's login credentials.

Disclaimer once configured can be edited but cannot be removed.

## Auto Purge on Expiry

Check to enable automatic purging of user details on expiry of user validity.



**Note:** Details of a user who is bound to rules (like firewall, IM, etc.) will not be purged automatically.

Username Prefix *	guest-
Group *	Guest Group
Password Length	8
Password Complexity	Alphanumeric Password
Disclaimer	
<input checked="" type="checkbox"/> Auto Purge on Expiry	

**Figure 160: Guest User General Settings**

- Specify the **Guest User Registration Settings**.

### Enable Guest Users Registration

Enable to allow secured Internet access to guest users.

### SMS Gateway

Select the gateway using which SMS should be sent.

Alternately you may add the SMS gateway from this page itself by clicking **Create new**.

### Guest Username

Select Use Cell Number as Username as method of generating a username.

If the **Guest Username** option is not selected, by default, the new user name will be generated with the value specified in **Username Prefix**.

### User Validity (Duration in Days)

Specify the validity of guest users in days.

### Default Country Code

Enable to configure a default country code.

The selected country is displayed as default option in the **Cell Phone Number** selection at the guest user registration page.

### CAPTCHA Verification

Select to enable or disable CAPTCHA (Completely Automated Public Turing Test To Tell Computers and Humans Apart) code verification on the guest user registration page to ensure the request is received for human being.

By enabling CAPTCHA verification, the user will be displayed a picture with characters that user must insert in a provided textbox below the picture. The administrator can therefore protect the device against attacks generated by automated programs.

Default: Enabled

The screenshot shows a configuration interface for guest user registration. At the top is a checkbox labeled "Enable Guest Users Registration". Below it is a section for "SMS Gateway" with a dropdown menu set to "SMS Gateway". Under "Guest Username", there is a checkbox "Use Cell Number As Username" and a field containing "7". Under "User Validity (Duration in Days)", there is a field containing "7". Under "Default Country Code", there is a dropdown menu labeled "Select Here". At the bottom is a section for "CAPTCHA Verification" with a checked checkbox "Enable". Each section has an information icon (a blue circle with an 'i') to its right.

**Figure 161: Guest User Registration Settings**

4. Click **Apply**.
5. Specify the **SMS Gateway**.

An SMS gateway allows sending and receiving short message service (SMS) to/from a home network for guest user registration. The device supports HTTP and HTTPS protocol based SMS service.

### Configure SMS Gateway

This page allows you to configure an SMS Gateway for guest user registration.

1. Go to **Configure > Authentication > Guest User Settings** and click **Add** under the **SMS Gateway** section.
2. Enter SMS gateway details.

#### Name

Enter the name of the SMS gateway.

#### URL

Specify the URL of the SMS gateway for sending an SMS request.

#### HTTP Method

Select the method for sending an SMS request to the SMS gateways from the options available:

**Available Options:** **Get:** Requests data from a specified resource. **Post:** Submits data to be processed to a specified resource.

#### Cell Number Format

Select to use country code with cell number.

#### Number Prefix

Specify the prefix value to be used with the cell number.

Number Prefix can include alpha-numeric and ASCII special characters.

It can be up to 4 characters long.

## Request Parameters

Specify the following request parameters to configure the SMS gateway.

### Name

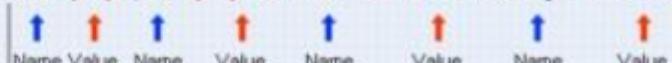
Name is a descriptor used to describe the meaning of the value. E.g. username, password, mobile

### Value

Indicates the value of a variable that are defined for the **Name**.

#### Example

```
HTTP://www.beat2day.co.in/sms.aspx?user=joey&pass=joey123&mbno=9876543210&msg=Test Message
```



Request Format

Name	Value
user	joey
pass	joey123
mbno	(mobileno)
msg	(msg)

Mobile number and message must follow "{mobileno}" and "{msg}" respectively.

## Response Format

Response describes the delivery status of the message such as success, failed, limit exceeded. Status message can be in various formats. Few of them are described below:

### Response Format

```
{0} | {1} | {2}
```

### Response Received

```
success | mbno | msgid/transactionid
```

### Response Format

```
<status>500</status><transactionid>{0}</transactionid><reason>{1}</reason>
```

### Response Received

```
<status>500</status><transactionid>2323</transactionid><reason>Limit Exceeded</reason>
```

When the response format is different for success and failure, it is recommended that the response format string should have a single content holder. E.g. {0}

## Response Parameters

Response Parameter is the value presented by the content holder {0,1,2...n} that will be displayed in the log viewer.

**Parameter Index:** Parameter Index is the content holder value {0,1,2...n}.

**Name:** Name represents the content holder in the log viewer.

Example 1:

Parameter Index	Name
0	Status
1	Recipient
2	SMSID

Example 2:

Parameter Index	Name
0	SMSID - 2323
1	SMS Status Message – Length Exceeded

The screenshot shows the configuration interface for adding an SMS gateway. It includes the following fields:

- Name \***: Enter Name (input field)
- URL \***: Enter URL (input field)
- HTTP Method \***: Radio buttons for Get (unselected) and Post (selected)
- Cell Number Format**: Checkboxes for Use Country Code with Cell Number (unchecked)
- Number Prefix**: Input field
- Request Parameters \***: Table with columns Name and Value. It has a '+' button to add new rows and a '-' button to remove existing ones.
- Response Format \***: Input field for Enter Response Format
- Response Parameters \***: Table with columns Parameter Index and Name. It has a '+' button to add new rows and a '-' button to remove existing ones.

**Figure 162: Add SMS Gateway**

- Click Save.

### Testing Connectivity with SMS Gateway

This page allows you to check connectivity with the gateway after you have configured an SMS gateway.

- Go to **Configure > Authentication > Guest User Settings** and in section **SMS Gateway**, edit the configured SMS gateway and click **Test Connection**.

2. Enter a cell phone number. You will receive SMS through the gateway configured if you are able to connect to the gateway.

The screenshot shows a configuration dialog box. At the top left is the label "Cell Phone Number \*". To its right is a text input field. Below the input field is a note: "Enter without a country code or \"0\" (Zero) as prefix e.g. 98XXXXXXXX". At the bottom of the dialog are two buttons: a blue "Save" button on the left and a white "Cancel" button on the right.

**Figure 163: Test Connectivity**

3. Click Save.

## Client Downloads

The **Client Downloads** page allows you to download all the clients or add-ins needed to interact with the device.

The device provides various options for user authentication. All the users are authenticated before they are provided access to network resources. User authentication can be performed using a local database, Active Directory, LDAP, RADIUS, TACACS, eDirectory, NTLM or combination of these. The device also supports Single Sign On (SSO) for transparent authentication whereby Windows credentials can be used to authenticate and the user has to login only once to access network resources. SSO can be used in Active Directory and Citrix or Terminal Services Environment.

Users can authenticate with the device using the Captive Portal, authentication clients for Windows, Linux, Macintosh, Android and iOS platforms or Single Sign On (SSO).

Following Clients can be downloaded from this page:

### Single Sign-On

**Sophos Single Sign-On Client** - Enables users to logon to the organization network as well as to the device simultaneously. This requires client installation on the user's machine.

**Sophos Transparent Authentication Suite (STAS)** - Enables transparent authentication whereby Windows credentials can be used to authenticate and the user has to login only once to access network resources. This does NOT require a client installation on the user's machine.

**Sophos Authentication for Thin Client (STAC)** - Enables transparent authentication for users in Citrix or Terminal Services Environment whereby network credentials can be used to authenticate and the user has to login only once to access network resources. This does NOT require a client installation on the user's machine.

### Authentication Clients

**Download MSI** - Enables admins to install authentication clients via Microsoft Installer to multiple user devices to access network resources and the Internet as per the policies configured in the device.

**Download CA for MSI** - Download the digital certificate to be installed via MSI to ensure a safe connection with the device.

**Download for Windows** - Enables users using a Windows operating system to logon to the device to access network resources and the Internet as per the policies configured in the device.

**Download for MAC OS X** - Enables users using a system with Macintosh OS X onwards to logon to the device to access network resources and the Internet as per the policies configured in the device.

**Download for Linux 32** - Enables users using a 32-bit Linux operating system to logon to the device to access network resources and the Internet as per the policies configured in the device.

**Download for Linux 64** - Enables users using a 64-bit Linux operating system to logon to the device to access network resources and the Internet as per the policies configured in the device.

**Download Certificate for iOS/Android client** - Download the digital certificate to be installed in an iOS or Android system to ensure a safe connection with the device. Authentication Clients for iOS/Android can be downloaded from the respective App Store/Play Store.

## SPX Add-ins

**This feature is available only with a valid Email Protection subscription**

**This feature is available in Sophos Firewall Models XG105 and above, Cyberoam Models CR25iNG and above, and all Sophos UTM Models.**

The **SPX Add-in** simplifies the encryption of the messages that contain sensitive or confidential information leaving the organization. The Add-in integrates seamlessly with the user's Microsoft Outlook software, making it easy for users to encrypt messages through the Sophos Firewall (SF) Email Protection.

Follow the steps given below to install the Add-in Outlook:

1. Unzip the files to a temporary folder.
2. For an interactive installation, run setup.exe (users will be prompted for input).
3. For an unattended installation, please note the following prerequisites.
  - Windows XP, Windows Vista, Windows 7, Windows 8 (both 32 and 64-bit) versions are supported.
  - Microsoft Outlook 2007 SP3, 2010 or 2013 (both 32 and 64-bit) versions are supported.

Now, proceed as follows:

- a. Install Microsoft .NET Framework 4 Client Profile.
- b. Install Microsoft Visual Studio 2010 Tools for Office Runtime 4.0.
- c. Run the installer with the following parameters: msixexec /qr /i SophosOutlookAddInSetupUTM.msi T=1 EC=3 C=1 I=1.

## STAS

This page describes how to configure the Sophos Transparent Authentication Suite (STAS).

Sophos Transparent Authentication Suite (STAS) enables transparent authentication whereby Microsoft Windows credentials can be used to authenticate. The user has to log in only once to access the network resources. A client installation on the user's machine is not required.

The Sophos Transparent Authentication Suite (STAS) program can be found under **Configure > Authentication > Client Downloads**. For more information about STAS installation, see [Sophos Transparent Authentication installation guide](#).

1. Go to **Configure > Authentication > STAS**.
2. To enable Sophos Transparent Authentication Suite click the toggle switch.
3. Click **Activate STAS**.
4. To enable the user inactivity click the toggle switch.
5. Specify the user inactivity.

### Inactivity Time

Specify the inactivity time in minutes. The user inactivity timeout is the inactive/idle time in minutes after which the user will be logged out and has to re-authenticate.

Acceptable range: 3 to 1440 minutes

Default: 3 minutes

### Data Transfer Threshold

Specify the minimum data to be transferred.

Default: 100 bytes

6. Click **Apply**.

## Related information

[How to implement Single Sign-On using STAS](#)

### Add New Collector

This page describes how to add a collector.

The STAS Collector collects user authentication requests from multiple agents, processes the requests and sends them to Sophos XG Firewall for authorization.

1. Go to **Configure > Authentication > STAS**.
2. Click **Add New Collector**.
3. Specify the collector details.

#### Collector IP

Enter a collector IP address.

#### Collector Port

Select collector port.

Default: 6677

#### Collector Group

Select a collector group. If you select **New Group** the collector will automatically be tagged with a group number. If you select **Existing Group** you can add the collector to an existing group.

Collector IP	Collector Port
<input type="text"/>	6677 <input type="button" value="▼"/>
Collector Group	
<input checked="" type="radio"/> New Group	<input type="radio"/> Existing Group

**Figure 164: Add New Collector**

4. Click **Save**.

### Disable STAS

This page describes how to disable STAS.

If you disable STAS, the current STAS configuration will be removed.

1. Click the toggle switch of the **Sophos Transparent Authentication Suite**.
2. Confirm deactivation by clicking on the **Confirm removal of STAS configuration** button.

## VPN

The VPN menu allows you to configure required IPsec, L2TP, PPTP and SSL VPN connections and connections with a CISCO™ VPN Client. Also, the section allows certificate and bookmark management required in the configured VPN connections.

A virtual private network (VPN) is a tunnel that carries private network traffic from one endpoint system to another over a public network such as the Internet without the traffic being aware that there are intermediate hops between the endpoints or the intermediate hops being aware they are carrying the network packets that are traversing the tunnel. The tunnel may optionally compress and/or encrypt the data, providing enhanced performance and some measure of security. VPN allows you to pretend you are using a leased line or a direct telephone call to communicate between the endpoints. VPNs allow users and telecommuters to connect to their corporate intranets or extranets. VPNs are cost-effective because users can connect to the Internet locally and tunnel back to connect to corporate

resources. This not only reduces overhead costs associated with traditional remote access methods, but also improves flexibility and scalability. For all business people traveling or working from home, connecting securely to the corporate network is essential. With the device, setting up a VPN is almost effortless.

The two endpoints in device VPN are referred to as:

- **Local** - First endpoint is the local machine itself.
- **Remote** - Second endpoint is the remote peer - the machine you are trying to establish a VPN connection to, or the machine which is trying to establish a VPN connection with you.

Device VPN automatically encrypts the data and sends it to the remote site over the Internet, where it is automatically decrypted and forwarded to the intended destination. By encrypting, the integrity and confidentiality of data is protected even when transmitted over the un-trusted public network. Device uses IPsec standard i.e. IPsec protocol to protect traffic. In IPsec, the identity of communicating users is checked with the user authentication based on digital certificates, public keys or preshared keys.

Device ensures that all the VPN traffic passing through the VPN tunnels is threat free. All the firewall rules and policies are applicable to the traffic going into the VPN tunnels and coming out of the VPN tunnels. Device inspects all the traffic passing through the VPN tunnels and makes sure that there are no viruses, worms, spam, and inappropriate content or intrusion attempts in the VPN traffic. As VPN traffic is by default subjected to the DoS inspection, the device provides a facility by which one can bypass scanning of traffic coming from certain hosts from a VPN zone. The above functionality is achieved by adding one additional zone called VPN zone. VPN traffic passes through the VPN zone and a firewall rule can be applied to the VPN zone.

Device can be used to establish VPN connection between sites, LAN-to-LAN and client-to-LAN connection. VPN is the bridge between local & remote networks/subnets.

Device supports following protocols to authenticate and encrypt traffic:

- Internet Protocol Security (IPsec)
- Layer Two Tunneling Protocol (L2TP)
- Point-to-Point Tunneling Protocol (PPTP)
- Secure Socket Layer (SSL)

## IPsec Connections

The **IPsec** menu allows you to create and manage IPsec connections and failover groups.

IP Security (IPsec) is a suite of protocols designed for cryptographically secure communication at the IP layer (layer 3).

IPsec protocols:

- **Authentication Header (AH)** – Used for the authentication of packet senders and for ensuring the integrity of packet data. The authentication header protocol (AH) checks the authenticity and integrity of packet data. In addition, it ensures that sender and receiver IP addresses have not been changed during transmission. Packets are authenticated using a checksum created by using a hash-based message authentication code (HMAC) in connection with a key.
- **Encapsulating Security Payload (ESP)** – Used for encrypting the entire packet and for authenticating its contents. In addition to encryption, ESP provides the ability to authenticate senders and verify packet contents.

This page contains two (2) sections:

1. [IPsec Connections](#)
2. [Failover Groups](#)

## IPsec Connections

The **IPsec Connections** section displays a list of all the IPsec connections. You can filter the list based on name, group name, policy name, connection type, and status of the connection. The page also provides the option to add a new connection, update the parameters of the existing policy, or delete a policy. In addition, you can create a

connection manually or through the connection wizard. In case of a remote access connection export the connection configuration by clicking the Export  icon under the Manage column.

 **Note:** You can also view and manage active IPsec connections on the **System > Current Activity > IPsec Connections** page.

The status of each connection is indicated as follows:

Connection Status	Description
Active	Connection
 	Connection is active but not connected. Click to initiate the connection.
 	Connection is active and connected. Click to disconnect the connection. When you disconnect, the connection will be deactivated. To re-establish the connection, activate the connection.
 	Connection is active but only partially connected. Click to disconnect the connection. When multiple subnets are configured for LAN and/or remote network, the device creates a sub-connection for each subnet. This status indicates that one of the sub-connections is not active.
 	Connection is inactive. Click to activate the connection.

## Failover Group

### Connection Failover

Connection Failover is a feature that enables you to provide an automatic backup connection for VPN traffic and provide “Always ON” VPN connectivity for IPsec connection. If the primary connection fails, the subsequent connection in the group will take over without manual intervention and keep traffic moving. The entire process is transparent to users.

### Connection Fallback

During a connection failure, the device checks the health of a primary connection every 60 seconds. When the primary connection is restored without the administrator’s intervention, the secondary connection fails back to the primary connection.

### Connection Failover Group

A VPN group is a grouping of IPsec connections. The phase 1 and phase 2 security parameters for each connection in a group can be different or identical except for the IP address of the remote gateway. The order of connections in the group defines the failover priority of the connection. Failover to the next connection will not occur if the group is manually deactivated.

The failover group containing the connection must be activated for the first time before participating in the failover. Failover to the next connection will not occur if the group is manually disconnected.

When the primary connection fails, the subsequent active connection in the group takes over without manual intervention and keeps traffic moving. For example, if the connection established using the 4th connection in the group is lost then the 5th connection will take over. Once the 4th connection is re-restored, the 5th connection will automatically fail back on the 4th connection.

The device considers a Site to Site and Host to Host connection as failed connection if the remote peer does not reply.

Connections that are not a part of the connection group do not participate in failover/fallback process and such connections will not be re-established automatically if lost.

To configure connection failover, you have to:

- Create connections.

- Create a failover group. A failover group is created by grouping all the connections that are to be used for failover. The order of connections in the group defines the failover priority of the connection.
- Define a failover condition.

### Prerequisites

- Packets of the protocol specified in the failover condition must be allowed from local server to remote server and its reply on both local and remote server
- One connection can only be member of single group
- Connection must be ACTIVE to participate in failover

### Procedure

1. Once the connection is added as a member of the group, DPD is configured as “Disable”, Key Negotiation Tries as 3, and Action on VPN Restart as “Disable”.
2. Once the connection is removed from the group, the original policy and connection configuration will be considered.
3. If the connection is already established at the time of adding it in the failover group, it will get disconnected.
4. On factory reset, failover configuration will not be retained.

The **Failover Group** section displays the list of created failover groups. You can filter or sort the groups based on group name. You can add a new group, update, or delete the group. In addition, the list displays the status of the group as:  indicating an activate group while  indicates an inactive group.

### Types of IPsec Connections

IPsec connection is the encrypted VPN connection established between two systems using the Internet protocol security (IPsec). It can link two hosts, two sites or remote user and a LAN.

The device supports following types of IPsec connections:

- **Remote Access** – This type of VPN is a user-to-internal network connection via a public or shared network. Many large companies have employees that need to connect to the internal network from the field. These field agents access the internal network by using remote computers and laptops without a static IP address.
- **Site to Site** – A Site to Site VPN connects an entire network (such as a LAN or WAN) to a remote network via a network-to-network connection. A network-to-network connection requires routers on each side of the connecting networks to transparently process and route information from one node on a local LAN to another node on a remote LAN.
- **Host to Host** – Host to Host VPN connects one desktop or workstation to another station by way of a host-to-host connection. This type of connection uses the network to which each host is connected to create a secure tunnel between the two.

### IPsec Connection Wizard

The IPsec Connection Wizard allows you to configure a VPN connection manually.

The wizard is not available if you are managing the device through Sophos Firewall Manager.

The VPN Connection Wizard takes you step-by-step through the configuration of a VPN connection on the device. After the configuration is completed, the wizard creates a new VPN connection.

Wizard is divided into two panels – Configuration panel and Help panel. Configuration parameters are to be entered in the Configuration panel while the Help panel on left-most side provides the help on the configuration parameters.

First screen of the wizard provides an overview of the configuration steps. You can create three types of connections through wizard:

- *Remote Access*
- *Site to Site*
- *Host to Host*

## Creating Remote Access Connection Using VPN Wizard

Go to **Configure > VPN > IPsec Connections**. Click **Wizard** and follow the steps given below.

Specify name and description (if required) for a VPN connection and click **Start**. The Help panel on left-most side provides an overview of each configuration step.

### On the Select a Connection Type page

1. Select the connection type **Remote Access**.
2. Select VPN policy to be applied to the connection traffic. Default policies as well as custom policies applicable to connection will be displayed.
3. Select action to be taken on the connection when VPN services or the device restart.

Available options:

- **Disable** – Connection will be disabled till the user activates it.
- **Respond Only** – Connection in ready state to respond to any incoming request.

4. Click **>** icon to continue.

### On the Authentication Details page

1. Select authentication type.

Available options:

#### Preshared Key

Specify the preshared key of minimum 5 characters. This preshared key will have to be shared or communicated to the peer at the remote end. At the remote end, the client will have to specify this key for authentication. Refer to the VPN client guide, Phase 1 Configuration.

If there is a mismatch in the key, the user will not be able to establish the connection.

#### Digital Certificate

Select local certificate that should be used for authentication by the device.

Select remote certificate that should be used for authentication by the remote peer.

2. Click **>** to continue.

### On the Local Network Details page

1. Select **Local WAN Port**. Selected port acts as an end-point of the tunnel.
2. Select **Local Subnet**. Select the local network(s) you wish to give access to remote users via this connection.
3. Select **Local ID**.

For **Preshared Key** and **Digital Certificate**, select any type of ID and enter its value. DER ASN1 DN (X.509) is not applicable.

For **Local Certificate**, the ID and its value configured in the local certificate are displayed automatically.

4. Click **>** to continue.

### On the Remote Network Details page

1. In the **Remote VPN Server** field specify the IP address or host name of the remote endpoint.  
To specify any IP address, enter \*.
2. Enable NAT traversal if a NAT device exists between your VPN endpoints i.e. when remote peer has private/non-routable IP address.
3. Select **Remote Subnet**. Select the remote network(s) that you wish to access via this connection. This option will be available only if NAT traversal is enabled.
4. Select **Remote ID**.

For **Preshared Key**, select any type of ID and enter its value. DER ASN1 DN (X.509) is not applicable.

In case of **Local Certificate**, the ID and its value configured in the local certificate are displayed automatically.

5. Click > to continue.

#### On the User Authentication page

1. Select **User Authentication Mode**.

Available options:

- **Disabled** – Choose if authentication is not required.
- **Enable as Client** – Enter username and password for authentication by the remote gateway.
- **Enable as Server** – Select all the users that are to be allowed to connect.

2. Click > to continue.

#### On the IPsec Connection Summary page

The page displays the settings with which the IPsec connection will be created.

Click **Finish** to create the IPsec connection or click < to go back to the previous page and change the settings.

### Creating Site to Site Connection using VPN Wizard

Go to **Configure > VPN > IPsec Connections**. Click **Wizard** and follow the steps given below:

Specify name and description (if required) for a VPN connection and click **Start**. The Help panel on left-most side provides an overview of each configuration step.

#### On the Select a Connection Type page

1. Select the connection type **Site to Site**.
2. Select VPN policy to be applied to the connection traffic. Default policies as well as custom policies applicable to connection will be displayed.
3. Select action to be taken on the connection when VPN services or the device restart.

Available options:

- **Disable** – Connection will be disabled until the user activates it.
- **Respond Only** – Connection is in ready state to respond to any incoming request.
- **Initiate** – Initiate to establish the connection every time VPN services or the device restart.

4. Click > icon to continue.

#### On the Authentication Details page

1. Select authentication type.

Available options:

##### Preshared Key

Specify the preshared key of minimum 5 characters. This preshared key will have to be shared or communicated to the peer at the remote end. At the remote end, the client will have to specify this key for authentication. Refer to the VPN client guide, Phase 1 Configuration.

If there is a mismatch in the key, the user will not be able to establish the connection.

##### Digital Certificate

Select local certificate that should be used for authentication by the device.

Select remote certificate that should be used for authentication by the remote peer.

**RSA**

Local RSA key is displayed which can be re-generated from the CLI console. Refer to the console guide for more details. Specify remote RSA key.

2. Click > to continue.

**On the Local Network Details page**

1. Select **Local WAN Port**. Selected port acts as an end-point of the tunnel.
2. Select **Local Subnet**. Select the local network(s) you wish to give access to remote users via this connection.
3. Select **Local ID**.

For **Preshared Key** and **RSA Key**, select any type of ID and enter its value. DER ASN1 DN (X.509) is not applicable.

For **Local Certificate**, the ID and its value configured in the local certificate are displayed automatically.

4. Click > to continue.

**On the Remote Network Details page**

1. In the **Remote VPN Server** field specify the IP address or host name of the remote endpoint.

To specify any IP address, enter \*.

2. Enable NAT traversal if a NAT device exists between your VPN endpoints i.e. when remote peer has private/non-routable IP address.
3. Select **Remote Subnet**. Select the remote network(s) that you wish to access via this connection. This option will be available only if NAT traversal is enabled.
4. Select **Remote ID**.

For **Preshared Key** and **RSA Key**, select any type of ID and enter its value. DER ASN1 DN (X.509) is not applicable.

In case of **Local Certificate**, the ID and its value configured in the local certificate are displayed automatically.

5. Click > to continue.

**On the User Authentication page**

1. Select **User Authentication Mode**.

Available options:

- **Disabled** – Choose if authentication is not required.
- **Enable as Client** – Enter username and password for authentication by the remote gateway.
- **Enable as Server** – Select all the users that are to be allowed to connect.

2. Click > to continue.

**On the IPsec Connection Summary page**

The page displays the settings with which the IPsec connection will be created.

Click **Finish** to create the IPsec connection or click < to go back to the previous page and change the settings.

**Creating Host to Host Connection using VPN Wizard**

Go to **Configure > VPN > IPsec Connections**. Click **Wizard** and follow the steps given below:

Specify name and description (if required) for a VPN connection and click **Start**. The Help panel on left-most side provides an overview of each configuration step.

**On the Select a Connection Type page**

1. Select the connection type **Host to Host**.
2. Select VPN policy to be applied to the connection traffic. Default policies as well as custom policies applicable to connection will be displayed.
3. Select action to be taken on the connection when VPN services or the device restart.

Available options:

- **Disable** – Connection will be disabled until the user activates it.
- **Respond Only** – Connection is in ready state to respond to any incoming request.
- **Initiate** – Initiate to establish the connection every time VPN services or the device restart.

4. Click > icon to continue.

#### On the Authentication Details page

1. Select authentication type.

Available options:

##### **Preshared Key**

Specify the preshared key of minimum 5 characters. This preshared key will have to be shared or communicated to the peer at the remote end. At the remote end, the client will have to specify this key for authentication. Refer to the VPN client guide, Phase 1 Configuration.

If there is a mismatch in the key, the user will not be able to establish the connection.

##### **Digital Certificate**

Select local certificate that should be used for authentication by the device.

Select remote certificate that should be used for authentication by the remote peer.

##### **RSA**

Local RSA key is displayed which can be re-generated from the CLI console. Refer to the console guide for more details. Specify remote RSA key.

2. Click > to continue.

#### On the Local Network Details page

1. Select **Local WAN Port**. Selected port acts as an end-point of the tunnel.

2. Select **Local ID**.

For **Preshared Key** and **RSA Key**, select any type of ID and enter its value. DER ASN1 DN (X.509) is not applicable.

For **Local Certificate**, the ID and its value configured in the local certificate are displayed automatically.

3. Click > to continue.

#### On the Remote Network Details page

1. In the **Remote VPN Server** field specify the IP address or host name of the remote endpoint.

To specify any IP address, enter \*.

2. Enable NAT traversal if a NAT device exists between your VPN endpoints i.e. when remote peer has private/non-routable IP address.

3. Select **Remote Subnet**. Select the remote network(s) that you wish to access via this connection. This option will be available only if NAT traversal is enabled.

4. Select **Remote ID**.

For **Preshared Key** and **RSA Key**, select any type of ID and enter its value. DER ASN1 DN (X.509) is not applicable.

In case of **Local Certificate**, the ID and its value configured in the local certificate are displayed automatically.

5. Click > to continue.

#### On the User Authentication page

## 1. Select User Authentication Mode.

Available options:

- **Disabled** – Choose if authentication is not required.
- **Enable as Client** – Enter username and password for authentication by the remote gateway.
- **Enable as Server** – Select all the users that are to be allowed to connect.

## 2. Click > to continue.

### On the IPsec Connection Summary page

The page displays the settings with which the IPsec connection will be created.

Click **Finish** to create the IPsec connection or click < to go back to the previous page and change the settings.

## Add VPN Failover Group

A VPN failover group enables you to have an always-on VPN connection. If the primary connection fails, the subsequent connection in the group will take over without manual intervention and keep traffic moving.

1. Go to **Configure > VPN > IPsec Connections**, scroll to the **Failover Group** section and click **Add**.
2. Type a name.
3. Select at least two connections.  
SF-OS selects the subsequent active connection from the list if the primary connection fails.
4. Enable mail notification to receive connection failure notifications.  
The email recipient is the one you entered during the network configuration.
5. Specify failover conditions.
6. Click **Save**.

## SSL VPN (Remote Access)

The SSL VPN (Remote Access) tab allows control of remote devices connected to your system.

The remote access SSL feature of Sophos XG Firewall is realized by OpenVPN, a full-featured SSL VPN solution. You can create point-to-point encrypted tunnels between remote employees and your company, requiring both SSL certificates and a username/password combination for authentication. This enables access to internal resources. In addition, a secure User Portal is offered, which can be accessed by each authorized user to download a customized SSL VPN client software bundle. This bundle includes a free SSL VPN client, SSL certificates and a configuration that can be handled by a simple one-click installation procedure. The SSL VPN client supports most business applications such as native Outlook, native Windows file sharing, and many more.

This page displays a list of all available remote policies. For each policy, the list shows:

### Name

Displays the name of the SSL VPN remote access policy.

### Use as Default Gateway

Displays if and which default gateway is used for the policy.

### Description

Displays the description which was entered for the policy.

<input type="checkbox"/> Name ▾	Use as Default Gateway ▾	Description	Manage
<input type="checkbox"/> userportal	Yes		 

**Figure 165: About SSL**

## Add SSL VPN Remote Access Policy

This page allows adding SSL VPN remote access policies.

1. Go to **Configure > VPN > SSL VPN (Remote Access)** and click **Add**.
2. Specify the **General Settings** details:

#### Name

Enter a unique name for the policy.

#### Description

Enter a description or other information.

The screenshot shows a form for 'General Settings'. It has two main sections: 'Name \*' with a text input field containing 'Enter Name' and 'Description' with a text input field containing 'Enter Description'.

**Figure 166: General Settings**

3. Specify the **Identity** details:

#### Policy Members

Click **Add New Item** to select available users/groups from a list or search for users/groups. When selected, click **Apply Selected Items**.



**Note:** You can also view and manage active SSL VPN users on the **Monitor & Analyze > Current Activities > Remote Users** page.

Selected items are displayed in the list. To remove an item from the list, click the Minus icon on the right of the item.

The screenshot shows a section titled 'Policy Members' with a large empty list area and a button below it labeled 'Add New Item'.

**Figure 167: Identity**

4. Specify the **Tunnel Access** details:

#### Use as Default Gateway

Activate the toggle switch if you want to use this as default gateway. If activated, all traffic is forwarded to a default gateway including external Internet requests. If deactivated, the traffic uses a split mode to separate traffic for internal network segments and external Internet requests through different gateways.

#### Permitted Network Resources (IPv4)

Click **Add New Item** to select available network resources from a list or search for network resources. When selected, click **Apply Selected Items**.

Selected items are displayed in the list. To remove an item from the list, click the Minus icon on the right of the item.

#### Permitted Network Resources (IPv6)

Click **Add New Item** to select available users/groups from a list or search for users/groups. When selected, click **Apply Selected Items**.

Selected items are displayed in the list. To remove an item from the list, click the Minus icon on the right of the item.

The screenshot shows the 'Permitted Network Resources' section. It has two main sections: 'Permitted Network Resources (IPv4)' and 'Permitted Network Resources (IPv6)'. Each section contains a large text input field and a 'Add New Item' button at the bottom.

**Figure 168: SSL VPN (Remote Access) Tunnel Access**

- Specify the **Idle Timeout** settings:

#### Disconnect Idle Clients

Activate/deactivate by clicking the toggle switch. If activated, clients which are idle will be disconnected from the session after a specified time.

#### Override Global Timeout (Default 15 Minutes) (*available only if Disconnect Idle Clients is selected*)

Enter a value for the idle timeout in minutes.

Acceptable range: 15 to 60 minutes

Default: 15 minutes

The screenshot shows the 'Idle Timeout' configuration. It includes a 'Disconnect Idle Clients' section with a 'ON' toggle switch and an 'Override Global Timeout (Default 15 Minutes)' section with an input field set to 'Minutes (15-60)'.

**Figure 169: SSL VPN (Remote Access) Idle Timeout**

- Click **Apply**.

New remote access policies immediately appear on the **SSL VPN (Remote Access)** list.



**Note:** For remote access connections to work check that **LAN** and **WAN** zones are activated for the User Portal on the **System > Administration > Device Access** page.

## SSL VPN (Site to Site)

The SSL VPN (Site to Site) tab allows you to establish secure Site-to-site VPN tunnels via an SSL connection.

SSL VPN connections have distinct roles attached. The tunnel endpoints act as either client or server. The client always initiates the connection, the server responds to client requests. Keep in mind that this contrasts with IPsec where both endpoints normally can initiate a connection.

### Server Connections

This section displays a list of all existing SSL VPN site-to-site server connections along with their status, connection name, connection, local and remote networks, received and sent bytes, and the date of connection. You can sort the list by the connection name, the local or remote networks. The list displays the status of each connection as follows:

#### Status

Indicates if the connection is active or not. You can activate/deactivate the connection by clicking the toggle switch.

#### Connection Name

Displays the name of the connection.

**Connection**

Indicates the status of the connection: online (green) or offline (red).

**Local Networks**

Displays the local networks that are allowed to be accessed remotely.

**Remote Networks**

Displays the remote networks that are allowed to connect to the local network(s).

**Bytes**

Indicates the number of bytes sent and received through this connection.

**Connected Since**

Displays the date the connection was established.

<input type="checkbox"/>	Status	Connection Name	▲	Connection	Local Networks	▼	Remote Networks	▼	Bytes	Connected Since	Manage
No Records Found											

**Figure 170: Server**

**Client Connections**

This section displays a list of all existing SSL VPN site-to-site client connections along with their status, connection name, connection, usage of HTTP proxy server, received and sent bytes. You can sort the list by the connection name and the usage of the HTTP proxy server. The page also provides options to add, edit, download or delete a connection. The list displays the status of each connection as follows:

**Status**

Indicates if the connection is activated or not. You can activate/deactivate the connection by clicking the toggle switch.

**Connection Name**

Displays the name of the connection.

**Connection**

Indicates the status of the connection: online (green) or offline (red).

**Use HTTP Proxy Server**

Displays the HTTP proxy server which is used for the connection.

**Bytes**

Indicates the number of bytes sent and received through this connection.

<input type="checkbox"/>	Status	Connection Name	▲	Connection	Use HTTP Proxy Server	▼	Bytes	Manage
No Records Found								

**Figure 171: Client**

**Add SSL VPN Site-to-Site Server Connection**

This page describes how to add a SSL VPN site-to-site server connection.

1. Go to **Configure > VPN > SSL VPN (Site to Site)** and click **Add** in the **Server** section.
2. Specify the server details:

**Connection Name**

Enter a descriptive name for the connection.

**Description**

Enter the description or other information.

### Use Static Virtual IP Address

Only select this option if the IP address pool is not compatible with the client's network environment: By default, clients are assigned an IP address from a virtual IP pool. Rarely, it may happen that such an IP address is already in use on the client's host. In that case, enter a suitable IP address in the **Static Peer IP** field which will then be assigned to the client during tunnel setup.

### Local Networks

Select or add one or more local networks to which remote network(s) are allowed to connect. If you create a new network, you can either add a single IP host or an IP host group.

### Remote Networks

Select or add one or more remote networks that are allowed to connect to the local network(s). If you create a new network, you can either add a single IP host or an IP host group.

The screenshot shows a configuration interface for adding an SSL server connection. It includes fields for:

- Connection Name \***: An input field labeled "Enter Connection Name".
- Description**: A text area labeled "Description".
- Use Static Virtual IP Address**: A checkbox labeled "Use Static Virtual IP Address".
- Local Networks \***: A list box with an "Add New Item" button.
- Remote Networks \***: A list box with an "Add New Item" button.

**Figure 172: Add SSL Server Connection**

**3. Click Save.**

The new SSL VPN site-to-site server connection appears on the **Server** list.

The next step is the client configuration which has to take place on client side and not on server side. Download the client configuration file with help of the provided button in the **Server** list.

**Note:** If you want to send the file via mail it is recommended to use the encryption option which is provided in the download dialog.

How to configure the client is described in the **Client** section.

### Add SSL VPN Site-to-Site Client Connection

This page describes how to add a SSL VPN site-to-site client connection.

**1. Go to Configure > VPN > SSL VPN (Site to Site) and click **Add** in the Client section.**

**2. Specify the client details:**

#### Connection Name

Enter a descriptive name for the connection.

#### Description

Enter the description or other information.

#### Configuration File

Browse for the client configuration file and click **Open**.

**Note:**

- The file has to be in *.apc* or *.epc* format.
- The file can be downloaded via the download icon in the **Manage** column of the server list on the **System > VPN > SSL VPN (Site to Site)** page.

**Password (*optional*)**

If the file has been encrypted, enter the password.

**Use HTTP Proxy Server (*optional*)**

Activate if the client is located behind a proxy server and enter the proxy settings:

- **Proxy Server:** Select or add a proxy server.
- **Proxy Port:** Enter a proxy port.
- **Proxy Requires Authentication:** Select the checkbox if the client needs to authenticate against the proxy and enter **Username** and **Password**.

**Override Peer Hostname**

Select the checkbox and add or select a **Hostname** if the server system's regular hostname cannot be resolved from the client host.

Connection Name *	<input type="text" value="Enter Connection Name"/>
Description	<input type="text" value="Description"/>
Configuration File	<input type="button" value="Browse..."/> No file selected. <span style="float: right;">File should be in .apc or .epc format</span>
Password	<input type="password" value="Password"/>
<input type="checkbox"/> Use HTTP Proxy Server <input type="checkbox"/> Override Peer Hostname	

**Figure 173: Add SSL Client Connection**

3. Click **Save**.

The new SSL VPN site-to-site client connection appears on the **Client** list.

**CISCO™ VPN Client**

This page describes how to configure an Cisco VPN client.

CISCO™ VPN Client is a software developed by CISCO that runs on Windows systems. It establishes encrypted VPN tunnels with highly secured remote connectivity for the remote workers.

1. Go to **Configure > VPN > Cisco VPN Client**.
2. Specify the **General Settings**.

**CISCO™ VPN Client**

Select to enable CISCO™ VPN Client.

All the fields will be available for configuration, once CISCO™ VPN Client is enabled.

Default: disabled.

**Interface**

Select an WAN port to act as endpoint.

IP Aliases created for WAN interfaces will be listed along with the default WAN interfaces.

**Authentication Type**

Select the authentication type.

Authentication of users depend on the connection type.

**Available Options:**

- **Preshared Key** - Preshared key authentication is a mechanism whereby a single key is used for encryption and decryption. Both peers should possess the preshared key. The remote peer uses the preshared key for decryption. On selecting this option the user has to provide:

- **Preshared Key** – Specify the preshared key to be used. The preshared key should be of minimum 5 characters.
- **Confirm Preshared Key** – Provide the same preshared key to confirm it.

This preshared key will have to be shared or communicated to the peer at the remote end. At the remote end, the client will have to specify this key for authentication. If there is a mismatch in the key, the user will not be able to establish the connection.

- **Digital Certificate**: Digital certificate authentication is a mechanism whereby sender and receiver both use a digital certificate issued by the certificate authority. Both sender and receiver must have each other's certificate authority.

- **Local Certificate** – Select the local certificate that should be used for authentication by the device
- **Remote Certificate** – Select the remote certificate that should be used for authentication by the remote peer.

**Local ID (*available only if Authentication Type selected is Preshared Key*)**

Specify a value for the local ID selected.

**Available Options:**

- DNS
- IP Address
- Email
- DER ASN1 DN (X.509)



**Note:** DER ASN1 DN(X.509) can not be used for **Preshared Key** authentication.

If **Digital Certificate** is selected, the ID and its value is displayed automatically as specified in the **Local Certificate**.

**Remote ID**

Select a value for the remote ID selected.

**Available Options:**

- DNS
- IP Address
- Email
- DER ASN1 DN (X.509)



**Note:** DER ASN1 DN(X.509) can not be used for **Preshared Key** authentication.

**Allowed User**

Select all the users who are to be allowed to connect to the configured CISCO<sup>TM</sup> VPN client.

The screenshot shows the 'General Settings' configuration for a Cisco™ VPN Client. The interface is titled 'CISCO™ VPN Client'. The 'Enable' checkbox is checked. The 'Interface' dropdown is set to 'PortB - 10.200.97.205'. The 'Authentication Type' dropdown is set to 'Preshared Key'. The 'Preshared Key' field contains '\*\*\*\*\*' with options to 'Change Preshared Key' or 'Show Preshared/PSK Key'. The 'Local ID' dropdown is set to 'Select Local ID' and has a text input field next to it. The 'Remote ID' dropdown is set to 'Select Remote ID' and has a text input field next to it. The 'Allowed User' dropdown lists three users: 'john.smith', 'alice.cooper', and 'sonam', each with a delete icon. A 'Add New Item' button is at the bottom of the list.

**Figure 174: General Settings****3. Specify the Client Information.****Name**

Enter a unique name for the connection.

**Assign IP from**

Specify the IP address range.

The device will lease the IP address to the Cisco™ IPsec client from the specified IP address range.

**Note:** Do not configure the above IP address range in L2TP or PPTP configuration.

**Allow leasing IP address from Radius server for L2TP, PPTP and CISCO VPN Client**

Click to lease the IP address to the L2TP, PPTP and CISCO VPN client users through the Radius server.

Radius is a protocol that allows network devices to authenticate users against a central database. It can also store technical information used by network devices.

If enabled, the configured IP address is overridden with the IP address provided by the Radius server.

**DNS Server 1**

Provide a DNS server IP address to be pushed to CISCO VPN clients.

**DNS Server 2**

Provide a DNS server IP address to be pushed to CISCO VPN clients.

The screenshot shows the 'Client Information' configuration page. The 'Name' field is set to 'HO\_TO\_IOS'. The 'Assign IP from' field shows a range from '10.202.143.75' to '10.202.143.85'. There is a checkbox for 'Allow leasing IP address from RADIUS server for L2TP, PPTP and CISCO VPN Client' which is unchecked. The 'DNS Server 1' and 'DNS Server 2' fields are empty.

**Figure 175: Client Information**

**4. Specify the Advanced Settings.**

**Disconnect when tunnel is idle**

Click to allow the device to delete an idle VPN session if it exceeds the specified idle session time interval.

**Idle session time interval (*available only if Disconnect when tunnel is idle option is enabled*)**

Specify the time limit after which an idle VPN session will be deleted by the device.

Acceptable Range: 120 to 999

**Apply**

Click to accept and save the Cisco VPN client configuration.

**Export Connection (*available only if a Cisco VPN connection is configured*)**

Click to export Cisco VPN client configuration.

Once the .tgb file has been exported, it has to be passed to the client.

On the client side, the client needs the Sophos IPsec client to import the .tbg file and establish a connection to Sophos XG Firewall.

The Sophos IPsec VPN client may be downloaded from <https://www.sophos.com/en-us/support/utm-downloads.aspx>.



**Note:** You cannot export the connection when an external certificate is selected as **Remote Certificate**.

**Reset**

Click to delete the entire Cisco VPN client configuration.

Disconnect when tunnel is idle
 Enable

Idle session time interval

Seconds (between 120-999)

**Figure 176: Advanced Settings**

## L2TP (Remote Access)

The **L2TP Connections** page displays a list of all the L2TP connections and you can sort the list based on the connection name. The page also provides the option to add a new connection, update existing connections, or delete a connection. The page displays the status of each connection as follows:

Connection Status	Description
Active	Connection  Connection is active but not connected. Click to initiate the connection.
	 Connection is active and connected. Click to disconnect the connection. When you disconnect, the connection will be deactivated and to re-establish the connection, click again to activate the connection.
Inactive	 Connection is inactive. Click to activate the connection.

### Add L2TP Connection

This page describes how to create an L2TP connection.

1. Go to **Configure > VPN > L2TP (Remote Access)** and click **Add**.
2. Specify the **General Settings**.

**Name**

Enter a unique name for the L2TP connection.

**Description**

Enter a description for the L2TP connection.

**Policy**

Select a policy to be used for the connection.

A new policy can be added by clicking **Create New**.

**Action on VPN Restart**

Select the action to be taken on the connection when VPN services or the device restart.

**Available Options:**

- **Respond Only** – Keeps the connection ready to respond to any incoming request.
- **Disable** – Keeps the connection disabled until the user activates it.

Name *	<input type="text" value="Connection Name"/>	
Description	<input type="text" value="Enter Description"/>	
Policy *	<input type="button" value="Default Policy"/>	
Action on VPN Restart *	<input type="button" value="Respond Only"/>	

**Figure 177: General Settings**

3. Specify the **Authentication Details**.

**Authentication Type**

Select the authentication type. Authentication of the user depends on the type of connection.

**Available Options:**

- **Preshared Key** – Preshared key authentication is a mechanism whereby a single key is used for encryption and decryption. Both peers should possess the preshared key. The remote peer uses the preshared key for decryption. On selecting this option the user shall has to provide the following details:

- **Preshared Key** – Specify the preshared key to be used. The preshared key should be of minimum 5 characters.
- **Confirm Preshared Key** – Provide the same preshared key to confirm it.

This preshared key will have to be shared or communicated to the peer at the remote end. At the remote end, the client will have to specify this key for authentication. If there is a mismatch in the key, the user will not be able to establish the connection.

- **Digital Certificate** – Digital certificate authentication is a mechanism whereby sender and receiver both use a digital certificate issued by the certificate authority. Both sender and receiver must have each other's certificate authority.

- **Local Certificate** – Select the local certificate that should be used for authentication by the device.
- **Remote Certificate** – Select the remote certificate that should be used for authentication by the remote peer.

The screenshot shows a configuration interface for authentication details. At the top, there is a dropdown menu labeled "Authentication Type \*". The option "Preshared Key" is selected. To the right of the dropdown is a blue information icon. Below the dropdown, there are two input fields: "Preshared Key \*" and "Confirm Preshared Key". Both fields contain the text "Preshared Key".

**Figure 178: Authentication Details**

#### 4. Specify the Local Network Details.

##### Local WAN Port

Specify the local port number that the local VPN peer uses to transport traffic related to TCP or UDP protocol.

Acceptable range: 1 to 65535

To specify any local port, enter \*.

##### Local ID (*available only if Authentication Type selected is Preshared Key*)

Select any type of ID from the available options and specify its value.

##### Available Options:

- DNS
- IP Address
- Email
- DER ASN1 DN (X.509)

Note: DER ASN1 DN (X.509) can not be used for Preshared Key authentication.

If Digital Certificate is selected, the ID and its value is displayed automatically as specified in the Local Certificate.

The screenshot shows a configuration interface for local network details. There are two dropdown menus. The first dropdown is labeled "Local WAN Port \*" and contains the value "PortB - 10.200.97.204". The second dropdown is labeled "Local ID" and contains the value "Select Local ID". Each dropdown has a blue information icon to its right. Below the dropdowns is a large empty text input field.

**Figure 179: Local Network Details**

#### 5. Specify the Remote Network Details.

##### Remote Host

Specify the IP address or hostname of the remote end-point. Specify \* for any IP address.

##### Allow NAT Traversal

Enable NAT traversal if a NAT device is located between your VPN endpoints i.e. when the remote peer has a private/non-routable IP address.

At a time only one connection can be established behind one NAT-box.

##### Remote LAN Network

Select an IP addresses and netmask of the remote network which is allowed to connect to the device server through a VPN tunnel. Multiple subnets can be specified. Select IP hosts from the list of IP hosts available on the Admin console.

You can also add a new IP host by clicking **Create New** or on **System > Hosts and Services > IP Host**.

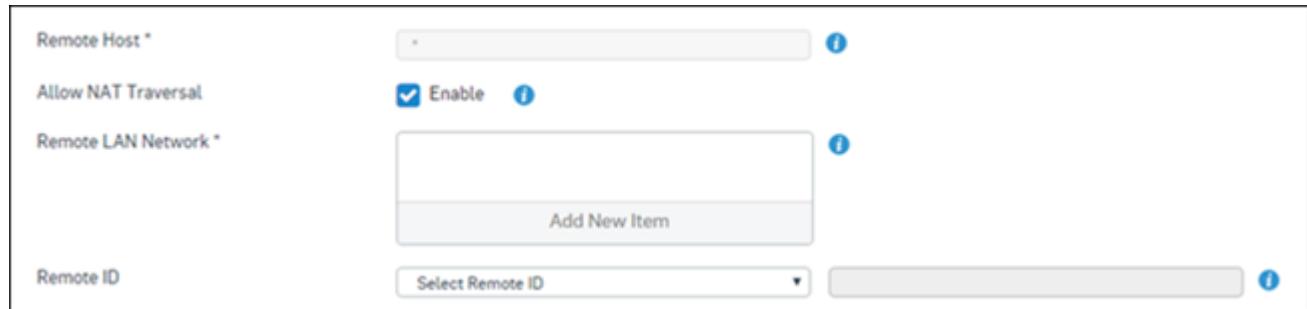
#### Remote ID

Select any type of ID from the available options and specify its value.

##### Available Options:

- DNS
- IP Address
- Email
- DER ASN1 DN (X.509)

 **Note:** DER ASN1 DN (X.509) can not be used for **Preshared Key** authentication.



The screenshot shows the 'Remote Host' configuration page. It includes fields for 'Remote Host' (with a dropdown menu), 'Allow NAT Traversal' (checked), 'Remote LAN Network' (with a dropdown menu and 'Add New Item' button), and 'Remote ID' (with a dropdown menu).

**Figure 180: Remote Network Details**

**6. Specify the Quick Mode Selectors.**

#### Local Port

Specify local port number that the local VPN peer uses to transport the traffic related to TCP or UDP protocol.

Default: 1701

Acceptable range: 1 to 65535

To specify any local port, enter \*.

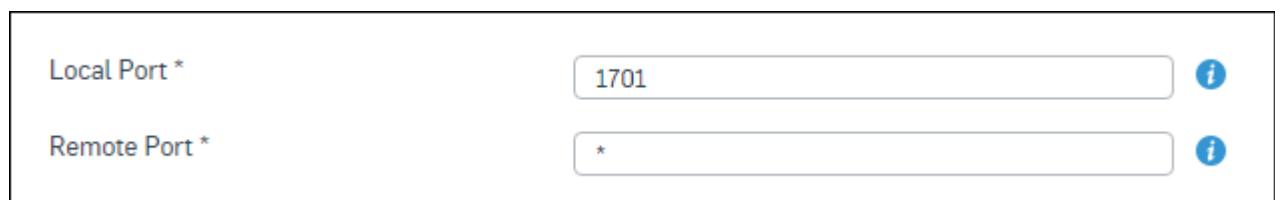
#### Remote Port

Specify remote port number that the remote VPN peer uses to transport the traffic related to TCP or UDP protocol.

Default: \*

Acceptable range: 1 to 65535

To specify any local port, enter \*.



The screenshot shows the 'Quick Mode Selectors' configuration page. It includes fields for 'Local Port' (set to 1701) and 'Remote Port' (set to \*).

**Figure 181: Quick Mode Selectors**

**7. Specify the Advanced Settings.**

#### Disconnect when tunnel is idle

Click this option to allow the device to delete an idle VPN session if it exceeds the specified idle session time interval.

**Idle session time interval (*available only if Disconnect when tunnel is idle is enabled*)**

Specify the time limit after which an idle VPN session will be deleted by the device.

Acceptable range: 120 to 999 seconds.

The screenshot shows a configuration page with a section titled "Advanced Settings". It contains two main items: a checkbox labeled "Disconnect when tunnel is idle" and a slider labeled "Idle session time interval". The slider has a range of "Seconds (between 120-999)".

**Figure 182: Advanced Settings**

8. Click Save.

## Clientless Access

Using clientless access, you can allow users to access services and areas on your network such as remote desktops and file shares using only a browser, and without the need for additional plug-ins. Clientless access policies specify users (members) and bookmarks. Users obtain access to your network through bookmarks on the VPN page in the user portal.

You can use this feature to provide multiple users access to resources that do not support multi-user access themselves (for example, network hardware) or constrain access to a specific service rather than providing access to entire systems or networks.

### Allowing Access to the User Portal From Outside Your Network

If you want to allow users outside your network to access the user portal, go to **System > Administration > Device Access** and specify WAN access.

### Clientless Access for Safari on Mac OSX or iOS

Follow the instructions in [How to access clientless bookmarks in iOS](#) to use clientless access on Safari on Mac OSX or iOS.

### Add a Clientless Access Policy

To be able to configure a policy, you need to create at least one bookmark.

1. Go to **Configure > VPN > Clientless Access** and click **Add**.
2. Type a name.
3. For **Policy Members**, click **Add New Item** and select the users or groups who should have access to the bookmarks.
4. For **Published Bookmarks**, click **Add New Item** and select bookmarks or bookmark groups.
5. Specify other settings as required.

Option	Description
<b>Restrict Web Applications</b>	When enabled, hide the <b>Secure Web Browsing</b> section in the user portal. This prevents users from being able to enter a URL and restricts them to the URLs specified in the bookmarks.

## Bookmarks

Bookmarks are connections that specify a URL, a connection type, and any required security settings. You can use bookmarks with clientless access policies to give users access to your internal networks or services. For example, you may want to provide access to file shares or allow remote desktop access. Users can access bookmarks through the VPN page in the user portal.

Bookmarks support several secure and non-secure connection types, or protocols.

## Add a Bookmark

1. Go to **Configure > VPN > Bookmarks** and click **Add**.
2. Type a name.
3. Select a type (protocol).

 **Note:** If you select a secure type, you must specify security settings.

<b>Option</b>	<b>Description</b>
<b>HTTPS</b>	Secure browser-based access to web applications using the Hypertext Transfer Protocol.  Bookmarks of this type support <i>referred domains</i> . These are domains or URLs that contain formatting information or scripts (for example, CSS or JavaScript) that are required to render the bookmarked URL appropriately.
<b>HTTP</b>	Non-secure browser-based access to web applications using the Hypertext Transfer Protocol.
<b>RDP</b>	Access to remote desktops using the Remote Desktop Protocol.  TLS, NLA, and RDP protocol security is supported. Your security settings must comply with the server settings.
<b>TELNET</b>	Terminal access using the Telnet protocol.
<b>SSH</b>	Secure terminal access using Secure Socket Shell.
<b>FTP</b>	Non-secure access to servers using the File Transfer Protocol.
<b>FTPS</b>	Secure access to servers using the File Transfer Protocol. Security is provided by TLS and SSL.
<b>SFTP</b>	Secure access to servers using the Secure File Transfer Protocol. Security is provided by SSH.
<b>SMB</b>	Access to servers using the Server Message Block file sharing protocol.
<b>VNC</b>	Remote access to Linux/UNIX hosts using Virtual Network Computing.  Classic VNC authentication (password only) is supported.

4. Type the URL of the website or the IP address of the server to which you want to provide access.

 **Note:** Changing the default port number is advisable for advanced users only.

5. Specify security settings as required.
  - For SSH: Specify a user name and paste the public host key.
  - For FTPS: Paste the public host key.
  - For SFTP: Type a user name and select an authentication method. Specify a password and paste keys as required.
6. Optionally, activate **Automatic Login** and specify credentials as required.

When enabled, users do not need to provide login credentials. The session will be established using the specified credentials.

If **Automatic Login** is disabled, authentication works as follows:

Option	Description
VNC	Users will be presented a dialog box asking for the VNC password.
RDP	Users will be presented a Windows login screen.
SMB	SF-OS tries to log in as guest user. For this to work, you must have set up the guest user account on the target server.
FTP(S)	Username “anonymous” and password “anonymous” is used.

- Specify other settings as required.

Option	Description
Share Session	When enabled, users can use the same connection simultaneously, allowing them to see the same screen.
Domain	Domain that the user is allowed to access.
Init Remote Folder	Remote directory. After successful authentication, the user is redirected to the specified folder on the remote server.

## Bookmark Groups

Bookmark groups allow you to combine bookmarks for easy reference. For example, you can create a group containing all of the bookmarks for remote desktops so that you do not need to specify access on an individual basis.

### Related tasks

[Add a Clientless Access Policy](#) on page 231

### Add a Bookmark Group

- Go to **Configure > VPN > Bookmark Groups** and click **Add**.
- Enter a name.
- Click **Add New Item** and select bookmarks.

**Figure 183: Add Bookmark Group**

The screenshot shows a form for adding a bookmark group. It includes fields for 'Name \*' (with a red asterisk), 'Description', and 'Select Bookmark \*' (with a red asterisk). Below the 'Select Bookmark' field is a large text area labeled 'Enter Description'. At the bottom right of the form is a button labeled 'Add New Item'.

## PPTP (Remote Access)

This page describes how to configure PPTP remote access.

The Point-to-Point Tunneling Protocol allows organizations to extend their own private network through private tunnels over the public Internet.

The device supports several authentication options including Password Authentication Protocol (PAP), Challenge Handshake Authentication Protocol (CHAP), and Microsoft Challenge Handshake Authentication Protocol (MS-CHAPv2).

The PPTP (Remote Access) page provides options to configure the device as PPTP server and enable/disable remote access through PPTP to various users.

1. Go to **Configure > VPN > PPTP (Remote Access)**.
2. Click to enable PPTP.
3. Specify the **General Settings**.

#### Assign IP from

Specify IP address range. PPTP server will lease IP address to the PPTP client from the specified IP address range. The PPTP client uses the assigned IP address as its source address for the duration of the connection.

Do not specify the same IP address range in L2TP configuration and PPTP configuration.

#### Allow leasing IP Address from Radius server for L2TP, PPTP and CISCO VPN Client

Click to lease the IP address to the PPTP users through the Radius server.

Radius server is a protocol that allows network devices to authenticate users against a central database. It can also store technical information used by network devices.

If enabled, the configured IP address is overridden with the IP address provided by the Radius server.

Assign IP from \*

Allow leasing IP address from RADIUS server for L2TP, PPTP and CISCO VPN Client i

**Figure 184: General Settings**

4. Specify the **Client Information**.

#### Primary DNS Server

Select the DNS server to be used at the client end.

#### Secondary DNS Server

Select the alternate DNS server to be used at the client end.

#### Primary WINS Server

Specify the WINS server to be used at the client end.

#### Secondary WINS Server

Specify the alternate WINS server to be used at the client end.

Primary DNS Server *	<input type="button" value="Select DNS Server"/>
Secondary DNS Server	<input type="button" value="Select DNS Server"/>
Primary WINS Server	<input type="text"/>
Secondary WINS Server	<input type="text"/>

**Figure 185: Client Information**

5. Click **Apply** to save the configuration.

6. Use the other buttons if required.

#### **Add Member(s) (*available only if PPTP is configured*)**

Click to select users who are to be allowed remote access through PPTP.

#### **Show Members (*available only if PPTP is configured*)**

Click to view a list of PPTP members.

#### **Related tasks**

[Add PPTP Member](#) on page 235

[PPTP Members](#) on page 235

### **Add PPTP Member**

The **Add PPTP Member** page allows you to select users who are to be allowed remote access through PPTP.

1. Go to **Configure > VPN > PPTP (Remote Access)** and click **Add Member(s)** to add users or user groups. A new window is displayed showing a list of users and user groups.
2. Select users or user groups who are to be allowed remote access through PPTP. You can add a single or multiple users or user groups.
3. Click **Apply** to add these users and user groups to the PPTP members list.

### **PPTP Members**

The **PPTP Members** page allows you to view list of PPTP members and remove members for whom remote access through PPTP is to be disabled.

1. Go to **Configure > VPN > PPTP (Remote Access)** and click **Show Members** to view a list of PPTP members. A new window is displayed showing a list of PPTP users who are allowed access through the PPTP connection.
2. Select the users for whom you want to disable PPTP access. You can select multiple users or user groups.
3. Click **Delete**.

## **IPsec Profiles**

This IPsec Profiles page displays a list of all preconfigured and custom IPsec policies.

A policy describes the security parameters used for negotiations to establish and maintain a secure tunnel between two peers.

Before you set up your secure tunnels, to make their configuration faster and easier, you can create VPN policies that work on a global level. Rather than configuring the policy parameters for every tunnel you create, you can configure general policies and then later apply them to your secure tunnels.

Click **Show Configuration** to show all configuration tabs.

#### **Authentication mode**

To ensure secure communication, there are two phases to every IKE (Internet Key Exchange) negotiation - Phase 1 (Authentication) and Phase 2 (Key exchange).

The Phase 1 negotiation establishes a secure channel between peers and determines a specific set of cryptographic protocols, exchanges shared secret keys and encryption algorithm that will be used for generating keys.

The Phase 2 negotiation establishes a secure channel between peers to protect data. During Phase 2 negotiation, the protocol security association for the tunnel is established. Either of the peers can initiate Phase 1 or Phase 2 renegotiation at any time. Both can specify intervals after which to negotiate.

#### **Key life**

Lifetime of key is specified as key life.

Once the connection is established after exchanging authenticated and encrypted keys, connection is not dropped till the key life. If the key life of both the peers is not same then negotiation will take place whenever the key life of any one peer is over. This means intruder has to decrypt only one key to break in your system.

Key generation and key rotation are important because the longer the life of the key, the larger the amount of data at risk, and the easier it becomes to intercept more ciphered text for analysis.

### **Perfect Forward Secrecy (PFS)**

It becomes difficult for a network intruder to get the big picture if keys are changing and they have to keep cracking keys for every negotiation. This is achieved by implementing PFS. By selecting PFS, new key will be generated for every negotiation and a new DH key exchange is included. So every time intruder will have to break yet another key even though he already knows the key. This enhances security.

### **Diffie-Hellman (DH) Group (IKE group)**

Diffie-Hellman is a public-key cryptography scheme that allows peers to establish a shared secret over an insecure communications channel. Diffie-Hellman Key Exchange uses a complex algorithm and public and private keys to encrypt and then decrypt the data.

The Diffie-Hellmann Group describes the key length used in encryption. Group number is also termed as Identifiers.

DH Group	Key length (bits)
1	768
2	1024
5	1536
14	2048
15	3072
16	4096

If mismatched groups are specified on each peer, negotiation fails. The group cannot be switched during the negotiation.

### **Re-key Margin**

Time before the next key is exchanged. Time is calculated by subtracting the time elapsed since the last key exchange from the key life. By turning Re-keying ‘Yes’, negotiation process starts automatically without interrupting service before key expiry.

### **Dead Peer Detection settings**

Use to check whether device is able to connect the IP Address or not. Set time interval after which the status of peer is to be checked and what action to take, if peer is not alive.

### **Tunnel Negotiation**

Negotiation process starts to establish the connection when local or remote peer wants to communicate with each other. Depending on the connection parameters defined, the key is generated which is used for negotiations. Lifetime of key is specified as Key life. Once the connection is established, connection is alive/active and data can be transferred up to the specified key life. Connection will be closed/deactivated once the key expires.

If the connection is to be activated again then the entire negotiation process is to be started all over again. Negotiation process can be started again automatically by either local or remote peer only if Allow Re-keying is set to ‘Yes’. Set the re-keying time in terms of the remaining key life when negotiation is to be started automatically without interrupting the communication before key expiry. For example, if key life is 8 hours and Re-key margin time is 10 minutes then negotiation process will automatically start after 7 hours 50 minutes of key usage.

Negotiation process will generate new key only if Perfect Forward Secrecy (PFS) is set to ‘Yes’. PFS will generate a new key from scratch and there will be no dependency between old and new key.

Re-keying	Result
Yes	Local and remote peer both will be able to initiate request for connection. Depending on PFS, negotiation process will use same key or generate a new key.
No	Only remote peer will be able to initiate request for connection. Depending on PFS, negotiation process will use same key or generate a new key.

Device provides 5 default policies and you can also create a custom policy to meet your organization’s requirement.

To make VPN connection configuration an easy task, following five preconfigured VPN policies are included for the frequently used VPN deployment scenarios:

- Road warrior
- L2TP
- Head office connectivity
- Branch office connectivity
- Default

It also provides option to add a new policy, update the parameters of an existing policy, or delete the policy. Instead of creating a policy from scratch, you can also create a new policy based on the already created policy by duplicating its parameters.

Duplicate - Click the  icon in the **Manage** column against the VPN Policy to be duplicated. The **Add VPN Policy** window is displayed which has the same values for parameters as the existing policy. Click **OK** to add a new policy with modification in values for parameters.

 **Note:** The default policy can be updated but cannot be deleted.

## Create a New IPsec Policy

This page describes how to quickly configure a new IPsec policy.

The **Add IPsec Policy** menu allows you to manually enter details to add a IPsec policy.

1. Go to **Configure > VPN > IPsec Profiles** and click **Add**.
2. Specify the **General Settings** details.

### Name

Enter a unique name for the IPsec policy.

### Description

Enter a description for the IPsec policy.

### Key exchange

Select an Internet Key Exchange (IKE) version to be used.

### Authentication Mode

Select an authentication mode. It is used for exchanging authentication information.

**Available Options:** **Main Mode** - Executes the Diffie-Hellman Key Exchange in three two-way exchanges. **Aggressive Mode** - Executes the Diffie-Hellman Key Exchange in one two-way exchange. A tunnel can be established faster as fewer messages are exchanged during authentication and no cryptographic algorithm is used to encrypt the authentication information. Use this option when the remote peer has dynamic IP addresses.

 **Note:** Aggressive Mode is insecure and, therefore, not recommended.

### Key Negotiation Tries

Specify maximum number of key negotiation trials. Set to 0 for unlimited.

#### Allow Re-keying

Enable re-keying to start the negotiation process automatically before the key expires. The negotiation can be initiated by the local or remote peer. Depending on PFS, the negotiation will use the same key or generate a new key.

#### Pass Data In Compressed Format

Enable to pass data in compressed format to increase throughput.

#### SHA2 with 96-bit truncation (available only for IKEv1)

Enable for truncation of SHA2 to 96 bits.

Name	Description
new Policy	Description
Key exchange	Key Negotiation Tries
<input checked="" type="radio"/> IKEv1 <input checked="" type="radio"/> IKEv2	5 Set 0 for unlimited number of negotiation tries
Authentication Mode	<input checked="" type="checkbox"/> Allow Re-keying
<input checked="" type="radio"/> Main Mode <input type="radio"/> Aggressive Mode	<input type="checkbox"/> Pass Data in Compressed Format
<small>⚠ Aggressive Mode is insecure</small>	<input type="checkbox"/> SHA2 with 96-bit truncation

**Figure 186: General Settings**

- Specify the **Phase 1** and **Phase 2** details.

#### Key Life

Lifetime of the key, in seconds.

#### Re-key Margin

Time, in seconds, of the remaining life of the key after which the negotiation process should be re-attempted. For example, if the key life is 8 hours, and the re-key margin is 10 minutes, the negotiation process will start after 7 hours and 50 minutes.

#### Randomize Re-Keying Margin by

Factor by which the re-keying margin is randomized. For example, if the key life is 8 hours, the re-key margin is 10 minutes, and the randomization is set to 20%, the negotiation attempts will start after 8 minutes and end at 12 minutes.

#### Algorithm

Combination of algorithms to use for encryption and authentication for the Diffie-Hellman Key Exchange. You can specify one or more combinations.



**Note:** The remote peer must be configured to use at least one of the defined algorithm combinations.

#### DH Group (Key Group)

Diffie-Hellman Group to use for encryption. The group specifies the key length used for encryption.



**Note:** The remote peer must be configured to use the same group.

#### Dead Peer Detection

Enable to check at specified interval to see whether peer is active.

#### Check Peer After Every (*only if the Dead Peer Detection option is enabled*)

Interval, in seconds, at which peer is checked.

#### Wait For Response Up to (*only if the Dead Peer Detection option is enabled*)

Time, in seconds, to wait for a peer response. If the response is not received within the specified interval, the peer is considered inactive.

**Action When Peer Unreachable (*only if the Dead Peer Detection option is enabled*)**

Specify the action to take when peer is determined to be inactive.

4. Click **Save**.

**SSL VPN**

This page describes how to configure general SSL VPN settings.

The SSL VPN tab allows you to define parameters requested for remote access such as protocols, server certificates and IP addresses for SSL clients. The SSL VPN client supports most business applications such as native Outlook, native Windows file sharing, and many more.

1. Go to **Configure > VPN > SSL VPN**.
2. Specify the SSL VPN Settings.

**Protocol**

Select the protocol to use. You can choose either **TCP** or **UDP**. UDP is recommended because it provides a better performance.

**SSL Server Certificate**

Select a local SSL certificate to be used by the SSL VPN server to identify itself against the clients.

**Default: ApplianceCertificate**



**Note:** The SSL VPN server does not support self-signed certificates that are not approved by a CA (which is not identical to the **Generate self-signed certificate** option in the Certificate section.)

**Override Hostname**

Here you can set the server IP address for client VPN connection. Usually this should be the external IP address of Sophos XG Firewall.

**IPv4 Lease Range**

Set an IP address range which is used to distribute IP addresses to the SSL clients. This should be a private IP address range.

Default Range: 10.81.234.5 to 10.81.234.55

**Subnet Mask**

Select a netmask for the IP address range above. The netmask must not be greater than 29 bits, because OpenVPN cannot handle address ranges whose netmask is /30, /31, or /32. The netmask is limited to a minimum of 16.

**IPv6 Lease (IPv6/Prefix)**

If you want to lease IPv6 addresses to clients, set the IPv6 prefix in the first field and the netmask in the last field.

You then also have to select the option **IPv4 and IPv6 both** in parameter **Lease Mode**.

**Lease Mode**

Select if you want to only lease IPv4 addresses to SSL clients or both IPv4 and IPv6 addresses.

**IPv4 DNS**

Specify up to two IPv4 DNS servers, primary and secondary, of your organization.

**IPv4 WINS**

Specify up to two IPv4 WINS servers, primary and secondary, of your organization.

Windows Internet Naming Service (WINS) is Microsoft's implementation of NetBIOS Name Server (NBNS) on Windows operating systems. Effectively, WINS is to NetBIOS names what DNS is to domain names—a central mapping of hostnames to IP addresses.

**Domain Name**

Enter the hostname of your Sophos XG Firewall as a Fully Qualified Domain Name (FQDN). The FQDN is an unambiguous domain name that specifies the node's absolute position in the DNS tree hierarchy, for example sf.example.com. A hostname may contain alphanumeric characters, dots, and hyphens. At the end of the hostname there must be a TLD (top level domain) such as com, org, or de. The hostname will be used in notification messages to identify the Sophos XG Firewall.

#### **Disconnect dead peer after**

Enter a time limit in seconds after which a dead connection will be terminated by Sophos XG Firewall.

Default: 180 seconds.

#### **Disconnect idle peer after**

Enter a time limit in minutes when an idle connection will be terminated.

Default: 15 minutes.

Protocol *	<input checked="" type="radio"/> TCP <input type="radio"/> UDP    (Select UDP for better performance)
SSL Server Certificate *	ApplianceCertificate
Override Hostname	
IPv4 Lease Range *	10.81.234.5 - 10.81.234.55 (Should be from Private IP ranges. First IP in the range will be used by the server.)
Subnet Mask *	/24 (255.255.255.0)
IPv6 Lease (IPv6/Prefix) *	2001:db8::1:0 / 64
Lease Mode *	IPv4 only
IPv4 DNS	Primary      Secondary
IPv4 WINS	Primary      Secondary
Domain Name	
Disconnect dead peer after *	180 Seconds (60 - 1800)
Disconnect idle peer after *	15 Minutes (15 - 60)

**Figure 187: SSL VPN Settings**

### **3. Specify the Cryptographic Settings.**

#### **Encryption Algorithm**

Specify the algorithm used for encrypting the data sent through the VPN tunnel. The following algorithms are supported and all in Cipher Block Chaining (CBC) mode:

- DES-EDE3-CBC
- AES-128-CBC (128 bit)
- AES-192-CBC (192 bit)
- AES-256-CBC (256 bit)
- BF-CBC (Blowfish (128 bit))

#### **Authentication Algorithm**

- SHA-1 (160 bit)
- SHA2 256 (256 bit)
- SHA2 384 (384 bit)
- SHA2 512 (512 bit)
- MD5 (128 bit)

#### **Key Size**

The key size (key length) is the length of the Diffie-Hellman key exchange. The longer this key is, the more secure the symmetric keys are. The length is specified in bits. You can choose between a key size of 1024 or 2048 bits.

#### Key Lifetime

Enter a time period after which the key will expire.

Default: 28,800 seconds

Encryption Algorithm	AES-128-CBC
Authentication Algorithm	SHA2 256
Key Size	2048 bit
Key Lifetime	28800 Seconds

**Figure 188: SSL VPN Cryptographic Settings**

- Specify the **Compression Settings**.

#### Compress SSL VPN Traffic

If enabled, all data sent through SSL VPN tunnels will be compressed prior to encryption.

- Specify the **Debug Settings**.

#### Enable Debug Mode

When enabling debug mode, the SSL VPN log file will contain extended information useful for debugging purposes.

- Click **Apply**.

## L2TP

This page describes how to enable and configure settings for L2TP connections.

Following is a description of the settings of this page:

- Go to **Configure > VPN > L2TP**.
- Click to enable L2TP.
- Specify the **General Settings**.

#### Assign IP from

Set an IP address range which is used to distribute IP addresses to L2TP clients. This should be a private IP address range.

#### Allow leasing IP address from RADIUS server for L2TP, PPTP and CISCO VPN Client

If this option is enabled and if the user is authenticated via a RADIUS server, the configured IP address (static or leased from the IP address range) is overridden with the IP address provided by the RADIUS server. If no IP addresses are configured on the RADIUS server, the static IP address configured for the user will be assigned, else an IP address will be leased from configured IP address range.

- Specify the **Client Information**.

#### Primary DNS Server

Select the DNS server to be used at the client end.

#### Secondary DNS Server

Select the alternate DNS server to be used at the client end.

#### Primary WINS Server

Specify the WINS server to be used at the client end.

#### Secondary WINS Server

Specify the alternate WINS server to be used at the client end.

5. Click **Apply** to save the configuration.
6. Use the other buttons if required.

#### **Add Member(s) (*available only if L2TP is configured*)**

Click to select users who are to be allowed remote access through L2TP.

#### **Show Members (*available only if L2TP is configured*)**

Click to view a list of L2TP members.

#### **Related tasks**

[Add L2TP Member](#) on page 242

[Show/Remove L2TP Member](#) on page 242

### **Add L2TP Member**

This page describes how to add an L2TP member.

Before you can add L2TP members, L2TP must be enabled. See chapter [L2TP](#) on page 241.

1. Go to **Configure > VPN > L2TP** and click **Add Member(s)** at the bottom of the page.
2. Select users and groups from the table who would use L2TP to connect to the device.
3. Click **Add**.

All selected entries will be added as L2TP members.

#### **Related tasks**

[L2TP](#) on page 241

This page describes how to enable and configure settings for L2TP connections.

[Show/Remove L2TP Member](#) on page 242

### **Show/Remove L2TP Member**

This page describes how to see which users or groups are members of L2TP and how to remove L2TP members.

Before you can view L2TP members, L2TP must be enabled. See chapter [L2TP](#) on page 241.

1. Go to **Configure > VPN > L2TP** and click **Show Members** at the bottom of the page.  
A dialog opens that shows all current members of L2TP.
2. Select users or groups from the table that should be removed as L2TP members.
3. Click **Delete**.

All selected entries will be removed as L2TP members.

#### **Related tasks**

[L2TP](#) on page 241

This page describes how to enable and configure settings for L2TP connections.

[Add L2TP Member](#) on page 242

## **Routing**

---

This section provides options to configure both static and dynamic routes.

Available configurations:

- [\*\*Static Routing\*\*](#) - Allows to configure packets redirection to a destination other than the configured default gateway.
- [\*\*Policy Routing\*\*](#) - Allows to configure Policy routes.
- [\*\*Gateways\*\*](#) - Allows to configure IPv4/IPv6 gateways.
- [\*\*BGP\*\*](#) - Allows to configure and manage BGP routes.

- *OSPF* - Allows to configure and manage OSPF routes.
- *Information* - Shows information and status of dynamic routes configured using RIP, OSPF, BGP or PIM-SM protocols.
- *Upstream Proxy* - Allows to configure parent proxy settings when the web traffic is blocked by the upstream gateway.
- *Multicast (PIM-SM)* - Allows to configure and manage PIM-SM routes.
- *RIP* - Allows to configure and manage RIP routes.

## Static Routing

A route provides the device with the information it needs to forward a packet to a particular destination. A static route causes packets to be forwarded to a destination other than the configured default gateway.

By specifying through which interface the packet will leave and to which device the packet should be routed, static routes control the traffic exiting the device.

### IP Multicast

Internet Protocol (IP) multicast is a bandwidth-conserving technology that reduces traffic by simultaneously delivering a single stream of information to thousands of recipients and homes. IP multicast delivers source traffic to multiple receivers without adding any additional burden on the source or the receivers.

Applications like videoconferencing, corporate communications, distance learning, and distribution of software, stock quotes, and news use IP multicasting.

If IP multicast is not used, the source is required to send more than one copy of a packet or individual copy to each receiver. In such case, high-bandwidth applications like video or stock where data is to be sent more frequently and simultaneously, uses large portion of the available bandwidth. In these applications, the only efficient way of sending information to more than one receiver simultaneously is by using IP multicast.

#### Multicast Group

Multicast is based on the concept of a group. An arbitrary group of receivers expresses an interest in receiving a particular data stream. This group does not have any physical or geographical boundaries - the hosts can be located anywhere on the Internet. Hosts that are interested in receiving data flowing to a particular group must join the group. Hosts must be a member of the group to receive the data stream.

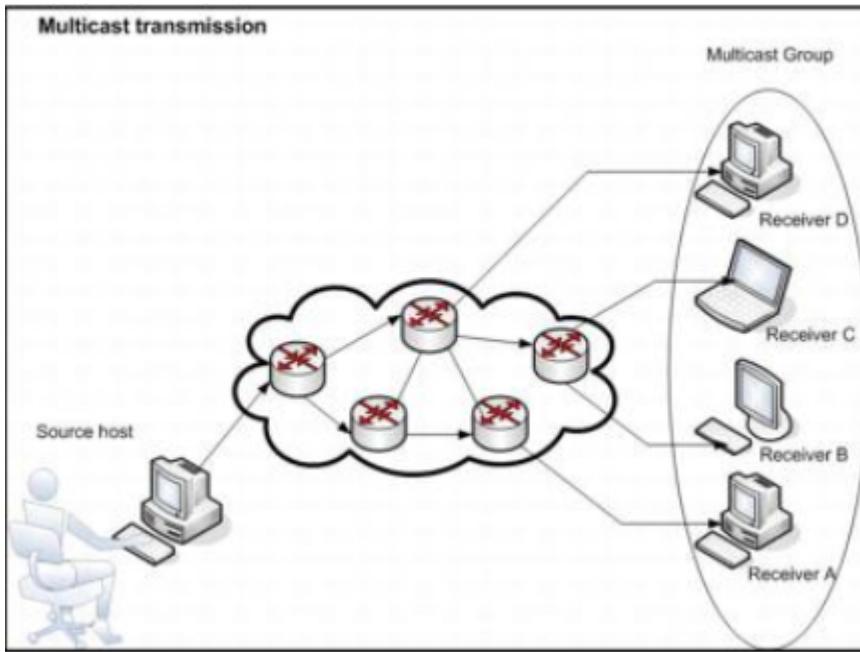
#### IP Multicast Addresses

Multicast addresses specify an arbitrary group of IP hosts that have joined the group and want to receive traffic sent to this group.

#### IP Class D Addresses

The Internet Assigned Numbers Authority (IANA) controls the assignment of IP multicast addresses. Multicast addresses fall in class D address space ranging from 224.0.0.0 to 239.255.255.255.

This address range is only for the group address or destination address of IP multicast traffic. The source address for multicast datagram is always the unicast source address.



### Multicast forwarding

With multicast forwarding, a router forwards multicast traffic to networks where other multicast devices are listening. Multicast forwarding prevents the forwarding of multicast traffic to networks where there are no nodes listening.

For multicast forwarding to work across inter-networks, nodes and routers must be multicast-capable.

A multicast-capable node must be able to:

- Send and receive multicast packets.
- Register the multicast addresses being listened to by the node with local routers, so that multicast packets can be forwarded to the network of the node.

IP multicasting applications that send multicast traffic must construct IP packets with the appropriate IP multicast address as the destination IP address. IP multicasting applications that receive multicast traffic must inform the TCP/IP protocol that they are listening for all traffic to a specified IP multicast address.

### Manage Static Routes

Static Routing menu allows configuring a unicast route and a multicast route. This page describes the available elements.

#### IPv4 Unicast Route

The IPv4 Unicast Route section displays a list of all the configured IPv4 unicast routes. You can filter the list based on IP address, gateway, or interface. The page also provides the option to **Add** a route, update the route configuration and **Delete** the route.

#### IPv6 Unicast Route

The IPv6 Unicast Route section displays a list of all the configured IPv6 unicast routes. You can filter the list based on IP address, gateway, or interface. The page also provides the option to **Add** a route, update the route configuration and **Delete** the route.

#### Multicast Forwarding Setting

##### Enable Multicast Forwarding

Enable/disable multicast forwarding. Enable and click **Apply** to allow the router to forward packets to other networks where other multicast devices are active and listening.

##### Manage Multicast Route

The Manage Multicast Route section displays a list of all the configured multicast routes. You can filter the list based on source IP, multicast IP, source interface and destination interface. The page also provides the option to **Add** a route, update the route configuration and **Delete** the route.

### Add Unicast Route

- For an IPv4 unicast route, go to **Configure > Routing > Static Routing** and click **Add** under **IPv4 Unicast Route**. For an IPv6 unicast route, click **Add** under **IPv6 Unicast Route**.
- Enter unicast route details.

#### Destination IP/Prefix

Specify the destination IPv4 or IPv6 address and select the prefix of subnet mask from the drop-down list.

#### Gateway

Specify the gateway IPv4 or IPv6 address. The gateway address specifies the next-hop router to which traffic will be routed.

#### Interface

Select an interface from the drop-down list.

#### Distance

Specify the distance for routing.

##### For IPv4

Default: 0

Acceptable Range: 0 to 255

##### For IPv6

Default: 1

Acceptable Range: 1 to 255

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

**Figure 189: IPv4 Unicast Route**

Destination IP * / Prefix *	<input type="text" value="Enter Destination IP"/> / <input type="text"/>
Gateway	<input type="text"/>
Interface	<input type="button" value="Select Interface"/>
Distance	1 (1-255)

**Figure 190: IPv6 Unicast Route**

- Click **Save**.

The unicast route has been created and appears on the **Static Routing** page.

### Add Multicast Route

- Go to **Configure > Routing > Static Routing** and click **Add** under **Manage Multicast Route**.
- Enter multicast route details.

#### Source IPv4 Address

Specify the source IPv4 address.

#### Source Interface

Select the source interface from the drop-down list.

#### Multicast IPv4 Address

Specify the multicast IPv4 address. For example, (224.0.2.0 - 239.255.255.255)

#### Destination Interface

Select destination interface(s) from the available options. You can select more than one destination interface.

Source IPv4 Address *	<input type="text" value="Enter Source IP Address"/>
Source Interface *	<input type="button" value="Select a Source Interface"/>
Multicast IPv4 Address *	<input type="text" value="(224.0.0.0 - 239.255.255.255)"/>
Destination Interface *	<input type="checkbox"/> PortA-10.198.15.35 <input type="checkbox"/> PortB-10.200.97.205 <input type="checkbox"/> PortC-192.168.1.40 <input type="checkbox"/> WWAN1 <input type="checkbox"/> IPsec Connection

**Figure 191: Add Multicast Route**

3. Click Save.

## Policy Routing

Routers generally forward packets to the destination addresses based on the information available in their routing tables. With Policy Routing, you can make routing decisions based on the policies configured by the administrator.

You can selectively forward the packets based on different criteria such as source network, destination network, services and so on. If the packet matches the criteria defined in the policy routing then the packet will be forwarded to the gateway configured in the policy.

Firewall Rule can still override policy route decision, if primary and/or backup gateway is configured.

#### Benefits of Policy Routing include:

- Packets originating from different source networks and having same destination can be routed to different networks.
- You can distribute traffic requiring high bandwidth to use different Internet connection.
- You can implement policies to achieve failover/failback. For example: If you have two links MPLS and VPN link and if MPLS link fails then you can route your traffic that matches the policy to VPN link. When the MPLS link comes up, then traffic can be failed back to MPLS link.

 **Note:** When device firmware is upgraded to SF-OS v16, source routes will be migrated as policy routes.

## Manage Policy Route

This page displays a list of all the configured IPv4 and IPv6 policy routes.

You can also reorder the policy routes. To change the processing order, you can reorder policy routes by drag and drop action. Policy routes are evaluated top down in the order they appear on the Manage page until first match is made, after which subsequent policy routes are not evaluated.

The page also displays the status Up  or Down  for the gateways configured in the policy route.

## Add Policy Route

1. Go to **Configure > Routing > Policy Routing** and click **Add** under **IPv4/IPv6 Policy Route** section.
2. Specify the Policy Route details.

### Name

Specify a name for policy route.

### Description

Specify a description for policy route.

The screenshot shows a form for adding a policy route. It has two main sections: 'Name \*' with a text input field labeled 'Enter Name' and 'Description' with a text input field labeled 'Enter Description'. Both fields have placeholder text: 'Enter Name' and 'Enter Description' respectively. There is a small 'x' icon in the bottom right corner of the description input field.

**Figure 192: About this Policy Route**

3. Specify the Traffic Selector details.

### Incoming Interface

Select the incoming interface receiving the packet.



**Note:** Deleting the incoming interface will also delete the policy route defined for the interface.

### Source Networks

Select the source network(s) of the packet to be routed. A new network host can be created directly from this page itself or from **System > Hosts and Services**.

### Destination Networks

Select the destination network(s) of the packet to be routed. A new network host can be created directly from this page itself or from **System > Hosts and Services**.

### Services

Select the services(s) of the packet to be routed. These services allow you to specify precisely which kind of traffic should be processed. A new service/service group can be created directly from this page itself or from **System > Hosts and Services**.

### DSCP Marking

Select the type of DSCP Marking to match the packets marked with the given DSCP value.

For available options, refer to [DSCP Values](#).

Incoming Interface	<input type="button" value="Select Interface"/>
Source Networks	<input type="button" value="Add New Item"/>
Destination Networks	<input type="button" value="Add New Item"/>
Services	<input type="button" value="Add New Item"/>
DSCP Marking	<input type="button" value="Select DSCP Marking"/>

**Figure 193: Traffic Selector**

4. Specify the Routing details.

#### Gateway

Select the gateway to which you want to forward the packet if the packet meets the configured matching criteria.



#### Note:

- Deleting the gateway will also delete the policy route defined for the gateway.
- Policy route is not applied when gateway goes down. As soon as the gateway comes up again, traffic is routed through the gateway automatically.

Gateway *	<input type="button" value="Select Gateway"/>
-----------	---

**Figure 194: Routing**

5. Click Save.

## Gateways

The Gateway page displays a list of configured IPv4 and IPv6 gateways. The page also displays the status Up or Down for each gateway. You can add/delete/clone gateway, change the gateway parameters/status and enable health check for the gateway.

#### Add a Gateway

1. Go to **Configure > Routing > Gateways** and click **Add**.
2. Enter Gateway details.

**Name**

Enter the name of the gateway.

**Gateway IP**

Enter the IP address of the gateway.

**Interface**

Select the Out interface for the gateway.

**Default NAT Policy**

Select the default NAT policy to be used for the gateway.

Select **None**, if NAT policy should not be applied on the gateway.

Name *	<input type="text"/>
Gateway IP	<input type="text"/>
Interface	<input type="text"/> None
Default NAT Policy	<input type="text"/> None 

**Figure 195: Gateway Host**

3. Enter Health Check details

**Health Check**

Click to enable health check for monitoring the gateway and specify the parameters based on the description shown below.

**Interval (in seconds)**

Specify the time interval in seconds after which the health should be monitored.

Acceptable Range: 5 to 65535 seconds

Default: 60 seconds

**Timeout (in seconds)**

Specify the time interval in seconds within which the gateway must respond.

Acceptable Range: 1 to 10 seconds

Default: 2 seconds

**Retries**

Specify the number of tries to probe the health of the gateway, after which the gateway will be declared unreachable.

Acceptable Range: 1 to 10

Default: 3

**Mail Notification**

Enable to receive an Email notification if there is a change in gateway status.



**Note:** You need to configure *Mail Server* for the device to send and receive alert Emails.

**Monitoring Condition**

**Protocol:** From the drop-down list, select the communication protocol, such as **TCP** or **PING** (ICMP). Select the protocol depending on the service to be tested for the gateway's health.

**Port:** For TCP communication, specify the port number for communication.

**IP Address:** Specify the IP address of the computer or the network device which is permanently running or most reliable.

## Operator:

- AND - All the conditions must be satisfied for the gateway to be considered alive.
  - OR - At least one condition must be satisfied for the gateway to be considered alive.

A protocol request is sent to the given IP address. If the IP address does not respond to the request within the timeout interval then given number of retries are attempted. If it still does not respond then the device considers the IP address as unreachable.

Health Check	<input checked="" type="checkbox"/>										
Interval *	<input type="text" value="60"/> [5-65535 seconds]										
Timeout *	<input type="text" value="2"/> [1-10 seconds]										
Retries *	<input type="text" value="3"/> [1-10]										
Mail Notification	<input type="checkbox"/> Enable										
Monitoring Condition	<table border="1"> <thead> <tr> <th>Protocol</th> <th>Port</th> <th>IP Address</th> <th>Operator</th> <th></th> </tr> </thead> <tbody> <tr> <td>PING</td> <td><input type="text"/></td> <td><input type="text"/></td> <td><input type="text"/></td> <td><input type="button" value="+"/></td> </tr> </tbody> </table>	Protocol	Port	IP Address	Operator		PING	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="button" value="+"/>
Protocol	Port	IP Address	Operator								
PING	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="button" value="+"/>							

**Figure 196: Health Check**

BGP

This page allows you to manage BGP routes.

Border Gateway Protocol (BGP) is a path vector protocol that contains path information, enabling the routers to share routing information between autonomous systems (AS) so that loop-free routes can be created. This protocol is generally used by ISPs.

An AS is a connected group of networks or routers under the control of single administrative entity and share common routing policies. A unique AS number is assigned to each AS to uniquely identify them. AS number enables information exchange between neighboring autonomous systems. You should use private AS numbers if you don't require a unique AS number. BGP private AS-numbers range from 64512 to 65535.

BGP selects a single path from the multiple advertisements received from multiple sources for the same route. When the path is selected, BGP puts it in the IP routing table and passes the path to its neighbor.

## Global Configuration

## Router ID

Specify router ID for BGP.

Example: 12.34.5.66.

Local AS

Specify Local Autonomous System (AS) number.

Acceptable Range: 1 to 4294967295

Router ID	<input type="text"/> (e.g. 12.34.5.66)
Local AS *	<input type="text"/> (1 - 4294967295)

**Figure 197: Global Configuration**

## Neighbors

Neighbors are the routers between which a TCP connection is established. In this section, you can [add](#), update, or delete neighbors.

## Networks

This section lists all available BGP networks together with their corresponding netmasks. You can [add](#), update, or delete networks.

### Add BGP Network

1. Go to **Configure > Routing > BGP** and click **Add** in the section **Networks**.
2. Enter the IPv4 address of the network and select a subnet mask from the dropdown list.

IPv4/Netmask *	<input type="text"/> / <input type="text" value="32 (255.255.255.255)"/>
----------------	--

**Figure 198: Add BGP Network**

3. Click **Save**.

### Add Neighbor

This page allows you to add a BGP neighbor and specify an IPv4 address of the neighbor router and AS number.

1. Go to **Configure > Routing > BGP** and click **Add** in the section **Neighbors**.
2. Specify the IPv4 address of the neighbor router.
3. Specify the remote autonomous system (AS) number of the neighbor.

Acceptable Range: 1 to 4294967295

IPv4 Address *	<input type="text"/>
Remote AS *	<input type="text"/> (1 - 4294967295)

**Figure 199: Add BGP Neighbor**

4. Click **Save**.

## OSPF

This page allows you to manage OSPF routes. You can also add, update, or delete the areas/networks/interface-specific configuration from this page.

Open Shortest Path First (OSPF) is an interior gateway protocol that multicasts the routing information to all the hosts within a single network. It sends routing information to all the routers in the network by calculating the shortest path to each router on the basis of the structure built up by each router.

OSPF allows sets of networks to be grouped together into what is known as areas. Area is a logical division of a network. Each area maintains a separate database whose information may be summarized by the connecting router. Hence, the topology of an area is not known to the outside world. There are three types of areas:

### **Backbone Area**

Backbone area also known as area 0, distributes information between non-backbone areas. All other areas in the network are connected to it and the routing between areas takes place using routers which are connected to the backbone area as well as to their respective areas.

### **Stub Area**

A stub area is an area that do not receive route advertisements external to the Autonomous System (AS), which is a collection of networks under a common network operator that share same routing policy.

### **NSSA**

A Not-so-stubby-area (NSSA) is a type of stub area that can import AS external routes in a limited amount.

### **Area Border Router**

An Area Border Router (ABR) is a router that connects areas to the backbone network and maintains separate routing information for each area that it is connected to. It has interfaces in more than one area with at least one interface in the backbone area.

## **Global Configuration**

### **Router ID**

Specify a unique router ID.

Example: 12.34.5.66.

Router ID	<input type="text"/>	(e.g. 12.34.5.66)
-----------	----------------------	-------------------

**Figure 200: Global Configuration**

### **Advanced Settings**

#### **Default Metric**

Specify the default metric value to be used for redistributed routes.

Metric is a property that contains a value used by a routing protocol to decide whether a particular route should be taken or not.

Default: 1

Acceptable Range: 1 to 16777214

#### **ABR Type**

Select the type of Area Border Router (ABR).

Available Options:

- Standard
- CISCO
- IBM
- Shortcut

#### **Auto cost reference bandwidth (Mbits/s)**

Specify the cost reference to calculate the OSPF interface cost based on bandwidth.

Default: 100 Mbits/s

Acceptable Range: 1 to 4294967

#### **Default Information Originate**

Select an option to control the distribution of the default route.

Available Options:

- Never
- Regular – On selecting **Regular** provide the metric and select the metric type.
- Always – On selecting **Always** provide the metric and select the metric type.

The default setting is **Never**.

#### **Redistribute Connected**

Click to enable the redistribution of connected routes into the OSPF routing table.

Specify the metric and the metric type for redistributing connected routes.

Acceptable Range: 0 to 16777214

Metric Type: **External Type 1** or **External Type 2**.

#### **Redistribute Static**

Click to enable the redistribution of static routes into the OSPF routing table.

Specify the metric and the metric type for redistributing static routes.

Acceptable Range: 0 to 16777214

Metric Type: **External Type 1** or **External Type 2**.

#### **Redistribute RIP**

Click to enable the redistribution of OSPF routes into OSPF routing table.

Specify the metric and the metric type for redistributing RIP routes.

Acceptable Range: 0 to 16777214

Metric Type: **External Type 1** or **External Type 2**.

#### **Redistribute BGP**

Click to enable the redistribution of BGP routes into the OSPF routing table.

Specify the metric and the metric type for redistributing BGP routes.

Acceptable Range: 0 to 16777214

Metric Type: **External Type 1** or **External Type 2**.

**Router ID**: (e.g. 12.34.5.66)

**Default Metric**: (0-16777214)

**ABR Type**: CISCO

**Auto cost reference bandwidth (Mbits/s)**: 100 (1-4294967)

**Default Information Originate**:  Never  Regular  Always

**Metric**: (0-16777214) **Metric Type**: External Type 2

**Redistribute Connected**:  Enable

**Metric**: (0-16777214) **Metric Type**: External Type 2

**Redistribute Static**:  Enable

**Metric**: (0-16777214) **Metric Type**: External Type 2

**Redistribute RIP**:  Enable

**Metric**: (0-16777214) **Metric Type**: External Type 2

**Redistribute BGP**:  Enable

**Metric**: (0-16777214) **Metric Type**: External Type 2

**Figure 201: Advanced Settings**

Click **Apply**.

## Networks and Areas

### Networks

This section lists all available OSPF networks together with the corresponding netmasks and the area they belong to.

### Areas

This section lists all available OSPF areas, specifies their types and authentication type, the area cost and, if available, virtual links.

### Override Interface Configuration

You can manage the interface configuration from this section.

### Add OSPF Areas

1. Go to **Configure > Routing > OSPF** and click **Add** in the **Areas** section.
2. Enter OSPF area details.

#### Area

Specify an IP address for the area.

#### Type

Select the type of OSPF area from the options available.

**Available Options:** Normal Stub Stub No-Summary NSSA No-Summary

#### Virtual Links (*Available only if Normal area type is selected*)

Specify a virtual link for an area that does not have a physical connection to connect to the backbone area.

Use Add icon  and Remove icon  to add and remove virtual links.

### Authentication

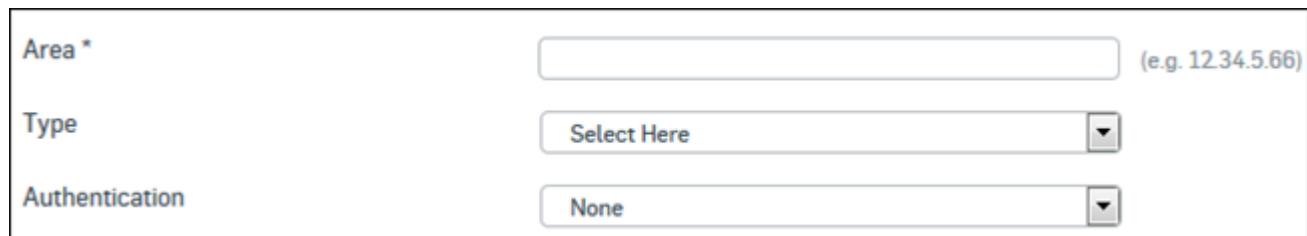
Select the type of authentication from the options available.

**Available Options:** TextMD5

### Area Cost (*Not Available for Normal area type*)

Specify the area cost.

Acceptable Range: 0 to 16777215



Area *	<input type="text" value=""/>	(e.g. 12.34.5.66)
Type	<input type="button" value="Select Here"/>	
Authentication	<input type="button" value="None"/>	

**Figure 202: Add OSPF Area**

3. Click Save.

### Add OSPF Network

1. Go to **Configure > Routing > OSPF** and click **Add** in the **Networks** section.
2. Enter the IPv4 address of the network and select a subnet mask from the dropdown list.
3. Enter an OSPF area.



IPv4/Netmask *	<input type="text" value="/32 (255.255.255.255)"/>	
Area *	<input type="text" value=""/>	(e.g. 12.34.5.66)

**Figure 203: Add OSPF Network**

4. Click Save.

### Override Interface Configuration

You can override default interface configurations of OSPF from this page.

1. Go to **Configure > Routing > OSPF** and click **Select Interface** in the **Override Interface Configuration** section.
2. Enter interface configuration details.

#### Interface

Select the interface to be configured for OSPF.

#### Hello Interval

Specify the time interval after which the interface sends hello packet to the neighbor router.

Default: 10 seconds

Acceptable Range: 1 to 65353 seconds

#### Dead Interval

Specify the time interval after which the interface is declared as dead.

Default: 40 seconds

Acceptable Range: 1 to 65353 seconds

### Retransmit Interval

Specify the time interval for retransmitting the link state advertisements (LSA) to the interface's neighbor.

Default: 5 seconds

Acceptable Range: 3 to 65353 seconds

### Transmit Delay

Specify the time in seconds needed to transmit a link state update packet to the interface.

Default: 1 second

Acceptable Range: 1 to 65353 seconds

### Interface Cost

Specify the interface cost.

You can either provide the interface cost automatically by selecting **Auto** or specify it manually.

Acceptable Range: 1 to 65353 seconds

### Authentication

Select the type of authentication for authenticating the OSPF packets.

**Available Options:** Text - If **Text** is selected, provide a password for authentication. MD5 - If **MD5** is selected, provide a key ID and a key. Key ID can be from 0 to 255.

### Router Priority

Specify priority for a router.

Default: 1

Acceptable Range: 0 to 255

Interface *	<input type="button" value="Select Here"/>
Hello Interval	10 (1-65535 seconds)
Dead Interval	40 (1-65535 seconds)
Retransmit Interval	5 (3-65535 seconds)
Transmit Delay	1 (1-65535 seconds)
Interface Cost	<input checked="" type="checkbox"/> Auto <input type="text"/> (1-65535)
Authentication	<input type="button" value="None"/>
Router Priority	1 (0-255)

**Figure 204: Override Interface Configuration**

3. Click Save.

## Information

Administrator can view various information and status of any dynamic routes configured using RIP, OSPF, BGP and PIM-SM protocols. This overview of the dynamic route information will be useful for further configurations and/or debugging.

## RIP Routes

Displays the entire routing configuration information and the routing table for an interface configured using the RIP protocol.

<b>Codes and Sub-codes</b>	Shows how the destination routing information is obtained.
<b>Codes</b>	R – RIP, C – connected, S – Static, O – OSPF, B – BGP, K – Kernel route.
<b>Sub-codes</b>	(n) – normal, (s) – static, (d) – default, (r) – redistribute, (i) – interface
<b>Network</b>	Specifies the IP address and subnet mask of the destination.
<b>Next Hop</b>	Specifies an IP address of the next hop routing device.
<b>Metric</b>	Specifies the number of routing devices (hop count) a packet must pass through to reach the final destination.
<b>From</b>	Indicates the router (router IP address) from which the metric is calculated to reach the destination.  If it is directly connected it will show <b>self</b> .
<b>Tag</b>	Indicates the method used for distinguishing between internal routes (learned by RIP) and external routes learned from External Gateway Protocol (ERP) protocols.  <b>0</b> indicates no tag is attached to the route.
<b>Time</b>	Indicates the elapsed time after which the routing entry will be flushed from the RIP table.
<b>Status</b>	Displays the RIP routing protocol process parameters and statistics.
<b>Routing Protocol is “rip”</b>	Indicates the routing protocol used.
<b>Sending updates</b>	Indicates the time between sending updates.
<b>Next due</b>	Specifies when the next update is due to be sent.
<b>Timeout after</b>	Indicates the timeout interval for RIP route after which it is declared invalid and removed from the routing table until the garbage-collect time expires.
<b>Garbage collect</b>	Indicates the time period during which the route metric is set to 16. If no updates are received for the route before the expiry of the garbage-

	collect timer, a route with metric 16 is deleted from the routing table.
<b>Outgoing update</b>	Indicates whether the outgoing filtering list has been set.
<b>Incoming update</b>	Indicates whether the incoming filtering list has been set.
<b>Default redistribution metric</b>	Metric of routes that are redistributed from other routes.
<b>Redistributing</b>	Indicates the information about redistribution of other protocols.
<b>Default version control</b>	Indicates the version of RIP packet that are sent and received.
<b>Interface</b>	Shows a RIP-enabled routing interface
<b>Send</b>	Displays the version of RIP packets sent out to the routing interface. The version is one of the following: RIP1, RIP2
<b>Recv</b>	Displays the version of RIP packets accepted on the routing interface. The version is one of the following: RIP1, RIP2 , Both
<b>Key-chain</b>	Displayed the authentication key-chain name for the interface, if it is configured.
<b>Routing for Network</b>	Indicates the networks for which the routing process is currently injecting routes.
<b>Routing Information Sources</b>	Indicates the routing sources used to build the routing table. For each source, the following information is displayed.
<b>Gateway</b>	Indicates an IP address of the next hop routing device.
<b>Bad Packets</b>	Indicates the number of bad packets received by the router.
<b>Bad Routes</b>	Indicates the number of invalid routes from the router.
<b>Distance Last Update</b>	Indicates the time when the administrative distance was last updated.
<b>Distance</b>	Indicates the administrative distance. The distance displayed by default is 120

**OSPF****Border Routers**

Displays the information about the internal OSPF routing table entries to an Area Border Router (ABR) and Autonomous System Boundary Router (ASBR).

<b>R</b>	Indicates that the information for the route is provided to a particular border router.
<b>Network IP Address</b>	Indicates the router ID of the destination.
<b>Metric</b>	Specifies the cost to reach the final destination.
<b>Area</b>	Indicates the area identifier of the outgoing interface.
<b>Next Hop</b>	Specifies the management IP address of the next hop routing device.
<b>Outgoing Interface</b>	Indicates the name and IP address of the outgoing interface to reach the destination.

**Routes**

Displays the information about the internal OSPF routing table entries.

<b>N</b>	Indicates that the information is provided for a network.
<b>Network IP Address</b>	Indicates the router ID of the destination.
<b>Metric</b>	Specifies the cost to reach the final destination.
<b>Area</b>	Indicates the area identifier of the outgoing interface.
<b>Next Hop</b>	Specifies the management IP address of the next hop routing device.
<b>Directly attached</b>	Indicates a network is directly connected to the interface.
<b>Outgoing Interface</b>	Indicates the name and IP address of the outgoing interface to reach the destination.

**Database**

Database shows the list of information related to the OSPF database summary for a specific router. Each link-state database includes link-state an advertisement from throughout the areas to which the router is attached.

<b>Link ID</b>	Indicates the ID of the link-state advertisement using which a router learns the route. In other words, while a link-state advertisement describes a router, the link-state ID router's OSPF router ID.
<b>ADV Router</b>	The link-state advertisement describing a network can have one of the following two formats of link-state ID: the network's IP address or an address generated using the link-state ID.
	Indicates the advertising router ID of the destination.

<b>Age</b>	Indicates the time, in seconds, since the LSA was generated.
<b>Seq#</b>	Link state sequence number (detects old or duplicate link-state advertisements).
<b>CkSum</b>	Checksum of the complete content of the link-state advertisement.
<b>Link count</b>	Number of interfaces detected for the router.
<b>Net Link States</b>	Gives information about network LSA originated by DR (designated router)
<b>Router Link States</b>	Gives information about router LSA originated by every router.
<b>Summary Net Link States</b>	Indicates the information about summary LSA originated by ABR's.

### **Neighbors (ARP - NDP)**

Provides neighbor information based on peer-interface relation.

<b>Neighbor ID</b>	Indicates the neighbor router's ID.
<b>Pri</b>	Indicates the router priority assigned to that neighbor.
<b>State</b>	Displays the conversation between router and neighbor since the neighbor was created. It can have one of the following values:
<b>Down</b>	Indicates the initial state of a neighbor conversation, that is, there has been no recent information received from the neighbor.
<b>Attempt</b>	Valid only for neighbors attached to non-broadcast networks. Indicates that there has been no recent information received from the neighbor.
<b>Init</b>	Indicates a hello packet has been received recently from a neighbor although the adjacency is not two-way, that is, a bi-directional communication has not yet been established with neighbor.

<b>2-Way</b>	Indicates that a bi-directional communication is established between the routers and the neighbor has included the router ID in its Hello message. The DR and BDR are elected from the set of neighbors in 2-way state or higher.
<b>ExStart</b>	Indicates that the two routers are going to synchronize and determine which router will be master and which the slave.
<b>Exchange</b>	Indicates that the two routers are describing their respective link-state database by sending database description packets.
<b>Loading</b>	Indicates that link-state request packets are sent to the neighbor, requesting for more advertisements that have been discovered but are not yet received in Exchange state.
<b>Full</b>	Indicates that both routers have accomplished the exchange of all the relevant advertisements and can now appear in router-link and neighbor-link advertisements.
<b>Backup</b>	Indicates that the neighbor is a backup designated router
<b>Dead time</b>	The waiting time in seconds to receive a hello message from OSPF neighbor before assuming the neighbor is dead.

<b>Address</b>	Specifies the IP address of the router's interface with the neighbor.
<b>Interface</b>	Indicates the IP address of neighbor interface
<b>RXmtL</b>	Indicates the link-state retransmit count.
<b>RqstL</b>	Indicates the link-state request count.
<b>DBsmL</b>	Indicates the link-state summary count.
<b>Interface</b>	Displays OSPF interface information.
<b>Interface Value</b>	Indicates the status of the physical interface, that is, whether the interface is up or down.
<b>IfIndex</b>	Indicates the value of interface index (IfIndex). It is an identification unique number associated with an interface.
<b>MTU</b>	Indicates the Maximum Transmission Unit (MTU) value of the interface.  MTU is the largest physical packet size, in bytes, that a network can transmit. This parameter becomes an issue when networks are interconnected and the networks have different MTU sizes. Any packets larger than the MTU value are divided (fragmented) into smaller packets before being sent.
<b>BW</b>	Indicates the bandwidth of the interface.
<b>Internet Address</b>	Displays the IP address of the interface.
<b>Network Type/IP Address</b>	Indicates the type of the network along with the IP address.
<b>Area</b>	Indicates the IP address of the area identifier.
<b>MTU mismatch detection</b>	Indicates whether the MTU mismatch detection is enabled or disabled. If it is enabled, it would match the MTU of both the interfaces participating in neighborship establishment.
<b>Router ID</b>	Indicates the identification number of the OSPF router selected at the start of the OSPF process. The router ID is unique within the OSPF domain and does not change unless OSPF restarts or is manually modified.
<b>Network Type</b>	Indicates the type of network to which the OSPF interface is connected. A network can be one of the following types:

<b>Point-to-point</b>	A point-to-point network can connect only two routers.
<b>Point-to-Multipoint (non-broadcast)</b>	A point-to-multipoint network connects one router to several other routers.
<b>Broadcast</b>	Indicates a network that supports broadcast. In a broadcast network a single packet sent (broadcasted) by a router is received by all the routers within the network.
<b>Non Broadcast Multiple Access (NBMA)</b>	Indicates that the network does not have the capability to broadcast or multicast. It is used to accurate model X.25 and frame-relay environment in multiple-access network.
<b>Cost</b>	<p>Displays the OSPF metric. It is calculated using formula: <math>10^8 / \text{bandwidth}</math> (in bits per seconds [bps]) where</p> <ul style="list-style-type: none"> <li>• <math>10^8</math>: is the reference bandwidth</li> <li>• bandwidth: is the bandwidth of the interface in bps</li> </ul>
<b>Transmit delay</b>	<p>Indicates the time in seconds which the OSPF router waits before flooding a link-state advertisement (LSA) over the link. The link state age is incremented by this value, before transmitting an LSA.</p> <p>The default value of transmit delay is 1 second.</p>
<b>State</b>	Indicates the current state of the specified interface. The state can be one of the following:
<b>DR</b>	The router is a designated router (DR) on the network.
<b>BDR</b>	The router is a backup designated router (BDR) on the network.
<b>DROTHER</b>	The router is neither a DR nor a BDR on the network

		and it establishes adjacencies only with the DR and the BDR.
<b>Waiting</b>	The interface router is in waiting to announce the state of the link as DR.	
		 <b>Note:</b> This state is normal in case of non broadcast multi access network.
<b>Point-to-Point</b>	The interface in point-to-point state is fully functional and starts exchanging hello packets with all its neighbors.	
<b>Point-to-Multipoint</b>	Indicates the interface to be point-to multipoint for OSPF.	
<b>Priority</b>	Indicates the priority of the interface router. It assists in electing the DR and BDR on the network to which the interface is connected. Default: 1	 <b>Note:</b> A router with priority value 0 can never be a DR/BDR.
<b>Designated Router ID</b>	Indicates the DR router ID for the respective network.	
<b>Backup Designated Router ID</b>	Indicates the BDR router ID for the respective network	
<b>Saved Network-LSA sequence number</b>	Indicates the network's link-state sequence number. It is used to calculate shortest path first (SPF).	
<b>Multicast group membership</b>	Indicates the multicast group in which the router is a member.	
<b>Timer intervals configured</b>	Displays the value of following OSPF timers:	
<b>Hello</b>	Time interval in seconds that a router sends a hello packet.	
<b>Dead</b>	Indicates the waiting time in seconds before declaring a neighbor dead.	
<b>Wait</b>	Displays the time interval that leads the	

		interface to terminate the waiting period and elect the DR on the network.
<b>Retransmit</b>	Displays the waiting time before re-transmitting a database description (DBD) packet if it has not been acknowledged earlier.	
<b>Hello Due In</b>	Specifies when the next hello packet is due to be sent.	
<b>Neighbor Count</b>	Indicates the total number of discovered neighbors on the interface.	
<b>Adjacent neighbor count</b>	Indicates the total number of adjacent neighbors that are fully adjacent to the interface.	

**BGP****Neighbors (ARP - NDP)**

Displays the information about the BGP and its peer connections and shows the number of routes advertised/neighbors to/from that peer.

<b>BGP Neighbor</b>	Indicates the IP address of the BGP neighbor.
<b>Remote AS</b>	Indicates the AS number of the neighbor router.
<b>Local AS</b>	Indicates the value of the configured local autonomous systems (AS).
<b>Internal/External Link</b>	Displays <b>internal links</b> for internal BGP (iBGP) neighbors and <b>external link</b> for external BGP (eBGP).
<b>BGP Version</b>	Indicates BGP version used for communication with remote router.
<b>Remote Router ID</b>	Indicates router ID of the neighbor router.
<b>BGP State</b>	Indicates the finite state machine (FSM) stage. It describes what action should be taken by the BGP routing engine and when for session negotiation.
<b>Last Read</b>	Displays the time, since BGP router last received a message from the neighbor. The time is displayed in HH:MM:SS format.
<b>Hold Time</b>	Displays the time in seconds, until which the BGP will maintain the session with the neighbor without receiving any message from it.

<b>Keepalive Interval</b>	Displays the time interval in seconds specifying how often the BGP router sends the keep-alive message to the neighbor.
<b>Message Statistics</b>	Displays the statistics organized by message type.
<b>InQ</b>	Indicates the number of messages that are in queue, pending to be processed from the neighbor.
<b>OutQ</b>	Indicates the number of messages that are in queue, pending to be sent to the neighbor.
<b>Sent</b>	Indicates the number of messages sent to the neighbor.
<b>Received</b>	Indicates the number of messages received from the neighbor.
<b>Opens</b>	Indicates the total number of open messages sent and received.
<b>Notifications</b>	Indicates the total number of error notification messages sent and received.
<b>Updates</b>	Indicates the total number of update messages sent and received.
<b>Keepalives</b>	Indicates the total number of keep-alive messages sent and received.
<b>Route Refresh</b>	Indicates the total number of route refresh messages sent and received.
<b>Capability</b>	Indicates the total number of BGP capabilities advertised and received from the neighbor.
<b>Total</b>	Indicates the total number of messages sent and received.

<b>Minimum Time between advertisement runs</b>	Displays the time in seconds between the sent advertisements.
<b>For Address Family</b>	Indicates the IP address family.
<b>Community attribute sent to this neighbor</b>	Indicates the numerical value of the BGP community.
	This numerical value is assigned to a specific prefix and advertised to the neighbor, based on which it decides whether to filter or modify attributes.
<b>Accepted Prefix</b>	Indicates the number of accepted prefixes that can participate in a BGP peer session.
<b>Connections established</b>	Indicates the number of times a TCP and a BGP connection has been established successfully.
<b>Dropped</b>	Indicates the number of times a valid session failed or has been taken down.
<b>Last reset</b>	Displays the time since when the previously established session with the neighbor ended.
<b>Local host and Local port</b>	Displays the IP address and port number of the local BGP router.
<b>Foreign host and Foreign port</b>	Displays the IP address of neighbor and BGP destination port number.
<b>Next hop</b>	Indicates the management IP address of the next hop routing device.
<b>Next connect timer due in</b>	Specifies when the next hello packet is due to be sent to the BGP neighbor.
<b>Read Thread</b>	Indicates if the read thread is ON or Off.
<b>Write Thread</b>	Indicates if the write thread is ON or Off.
<b>Routes</b>	Displays the entire routing configuration information and the routing table for an interface configured using the BGP protocol.
<b>BGP Table Version</b>	Indicates the table version number. The version number is updated with any change in the BGP table.
<b>Local Router ID</b>	Indicates the IP address of the router.
<b>Status codes and Origin codes</b>	Shows how the destination routing information is obtained.  <b>Status Codes:</b> A Status code indicates the status of the table entry and is displayed at the beginning of each line in the table. Status code value can be one of the following: s – suppressed, d –damped, h – history, * – valid, > – best, i – internal, r – Routing Information Base (RIB)-failure, S – Stale, R – Removed.  <b>Origin codes:</b> An Origin code indicates the origin of the entry and is displayed at the end of

	each line in the table. Origin code value can be one of the following: i – Interior Gateway Protocol (IGP), e – Exterior Gateway Protocol (EGP), ? – incomplete/path not clear.
<b>Network</b>	Indicates the IP address and subnet mask of the destination.
<b>Next Hop</b>	Indicates the management IP address of the next hop routing device. 0.0.0.0 indicates the router has non-BGP routes to the network.
<b>Metric</b>	Indicates the value of inter autonomous system metric.
<b>LocPrf</b>	Indicates the local preference value. Local preference is one of the methods to change the path taken by one autonomous system (AS) to reach to another AS. Local preference value indicates to AS about the path that has local preference, and one with the highest preference being preferred.
<b>Weight</b>	Indicates the route weight as set via autonomous system filters. If more than one path exists to a particular IP address, then the path with the highest weight is selected.
<b>Path</b>	Indicates the autonomous system path to the destination network.
<b>Total number of prefixes</b>	Indicates the total number of prefixes/networks.

### Summary

Displays the status of all the BGP connections details such as path, prefixes and attributes information about all the connections to BGP neighbors.

<b>BGP Router Identifier</b>	Indicates the router ID of the BGP router
<b>Local AS Number</b>	Indicates the local autonomous system number to which this router belongs.
<b>RIB entries</b>	Indicates the number of routing information entries in RIB
<b>Memory</b>	Indicates the memory used by RIB entry/ies.
<b>Peer</b>	Indicates the number of neighbors with which the connection is established.
<b>Memory</b>	Indicates the memory used by neighbor entries.
<b>Neighbor</b>	Indicates the IP address of the neighbor.
<b>V</b>	Indicates BGP version number provided to the neighbor.
<b>LocPrf</b>	Indicates local preference value.

<b>AS</b>	Local preference is one of the methods to change the path taken by one autonomous system (AS) to reach to another AS.
<b>MsgRcvd</b>	Local preference value indicates to AS about the path that has local preference, and one with the highest preference being preferred.
<b>MsgSent</b>	Indicates the number of messages sent to the neighbor.
<b>TblVer</b>	Indicates the last version of the BGP database that was sent to the neighbor.
<b>InQ</b>	Indicates the number of messages that are in queue, pending to be processed from the neighbor.
<b>OutQ</b>	Indicates the number of messages that are in queue, pending to be sent to the neighbor.
<b>Up/Down</b>	Indicates the total time of a BGP session to remain in established state, or gives the current status of BGP session, if it is not in established state.
<b>State/PfxRcd</b>	Indicates the state of the neighbor and the number of prefixes received.
<b>Total number of neighbors</b>	Indicates the total number of neighbors.

### PIM-SM

#### Interface Table

Displays all the PIM enabled interfaces and the neighbor information of each interface.

#### Multicasting Routing Table

Displays the information of the multicast groups joined. The information includes the source address, multicast group address, the incoming interface from which packets are accepted, list of outgoing interfaces to which packets are sent, PIM timers, flag bits etc.

#### RP SET

Displays RP set information which is a collection of group-to-RP mappings. This information is used to determine the RP for a multicast group and is maintained by a PIM router.

## Upstream Proxy

If your enterprise contains numerous internal branches, an upstream proxy can bundle the requests from the internal network before passing the traffic on to the external network/Internet.

This page allows you to configure an upstream proxy for IPv4/IPv6.

### IPv4 Parent Proxy

#### Parent Proxy

Click to enable the parent proxy, if the web traffic is intercepted by an upstream gateway.

If enabled, the device forwards all the HTTP requests to the parent proxy server.

**Domain Name/IPv4 Address**

Specify a domain name or IPv4 address for the parent proxy.

**Port**

Specify the port number, which is to be used for the parent proxy.

Default: 3128

**Username**

Specify a username for authentication.

**Password**

Specify a password for authentication.

<b>Parent Proxy</b>	<input type="checkbox"/> <b>Enable</b>
<b>Domain Name/IPv4 Address *</b>	<input type="text"/>
<b>Port *</b>	<input type="text" value="3128"/>
<b>Username</b>	<input type="text"/>
<b>Password</b>	*****

**Figure 205: IPv4 Parent Proxy**

Click **Apply**.

**IPv6 Parent Proxy****Parent Proxy**

Click to enable the parent proxy, if the web traffic is intercepted by an upstream gateway.

If enabled, the device forwards all the HTTP requests to the parent proxy.

**Domain Name/IPv6 Address**

Specify a domain name or IPv6 address for the parent proxy.

**Port**

Specify the port number to be used for the parent proxy.

Default: 3128

**Username**

Specify a username for authentication.

**Password**

Specify a password for authentication.

Parent Proxy	<input type="checkbox"/> Enable
Domain Name/IPv6 Address *	
Port *	3128
Username	
Password	*****

**Figure 206: IPv6 Parent Proxy**

Click **Apply**.

## Multicast (PIM-SIM)

This page allows you to configure PIM.

Protocol Independent Multicast (PIM) is a protocol for routing IP packets efficiently to multicast groups that may span throughout the Internet. PIM provides dynamic multicast support on the device. With dynamic multicast support, a host can join/leave a multicast group dynamically and there is no need to manually add/delete multicast routing entries on the device.



**Note:** The device supports PIM version2 and PIM-SM mode with Rendezvous Point (RP) selection method as BSR (Bootstrap Router)

### PIM-SM Configuration

#### Enable PIM

Enable PIM to provide dynamic multicast support on the device.

#### PIM Enabled Interface

Select the physical interfaces on which PIM service needs to be enabled.

To enable PIM, at least one interface has to be selected.



#### Note:

- Only IPv4 bound interfaces can be selected.
- Alias, PPPoE and Cellular WAN interfaces are not supported.

<input type="checkbox"/> Enable PIM
PIM Enabled Interface
<input type="button" value="Add New Item"/>

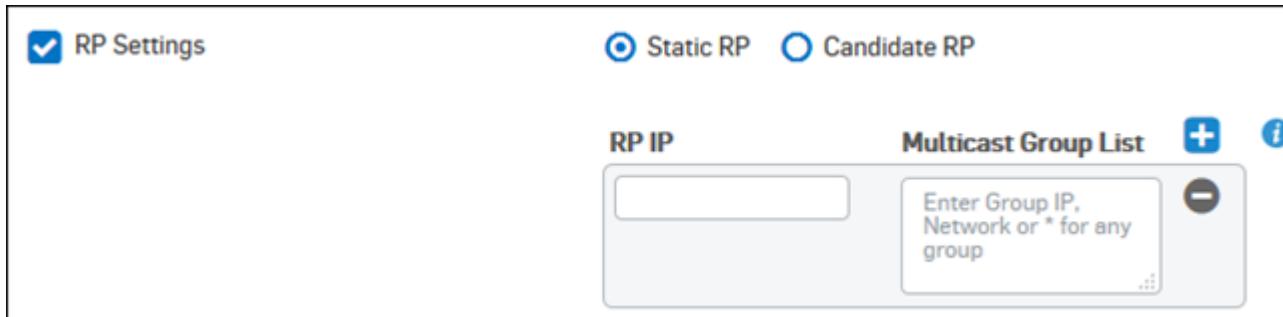
**Figure 207: PIM-SM Configuration**

#### RP Settings

Enable to configure Static RP or Candidate RP.

#### Static RP

<b>RIP IP</b>	Specify a unicast IP address for static RP. RPs can be added or deleted. Maximum eight RP IP addresses per RP are allowed.
<b>Multicast Group</b>	Specify Multicast Group IP address or network address separated by comma that will be served by given RP. Maximum eight multicast group addresses per RP are allowed Use * in <b>Multicast Group List</b> to serve all the multicast groups by the defined RP.



**Figure 208: Static RP Settings**

#### Candidate RP

**Candidate RP IP** Select interface IP that will be used as RP IP, if the router is selected as candidate RP.

**Multicast Group List** Specify multicast group IP address or network address separated by a comma that will be served by given RP.

Maximum eight multicast group IP/network addresses are allowed.

Use \* in **Multicast Group List** to serve all the multicast groups by the selected RP.

#### Candidate RP Priority

Specify the priority of the PIM router in the RP election process.

Default: 1

Acceptable Range: 1 to 255

#### Timer

Specify time in seconds after which at every specified time, RP candidate messages are generated.

Default: 60 seconds

Acceptable Range: 30 to 180 seconds

The screenshot shows the 'Candidate RP Settings' section of a configuration interface. At the top, there are three radio buttons: 'RP Settings' (selected), 'Static RP', and 'Candidate RP'. Below these, under the 'Candidate RP' section, there is a dropdown menu for 'Candidate RP IP', a text input field for 'Multicast Group List' with a placeholder 'Enter Group IP, Network or \* for any group', a text input field for 'Candidate RP Priority' with a value of '1' and a range of '(1-255)', and a text input field for 'Timer' with a value of '60' and a range of '(30-180)'.

**Figure 209: Candidate RP Settings**

## RIP

This page allows you to manage RIP routes. You can also add, update, or delete the networks/interface-specific configuration from this page.

Routing Information Protocol (RIP) is a widely used routing protocol that uses hop count to determine the best route to a destination.

RIP avoids routing loops from continuing indefinitely by limiting the number of hops permitted between the source and destination. The maximum number of hops supported is 15. Hence, if the hop count becomes 16, it is known as an infinite distance and is considered as unreachable.

With the help of the RIP protocol, the device sends routing update messages at regular intervals to the next router. When the next router receives the changes, it updates them in the routing table and also increases the metric value for the path by 1. The sender of the message is considered as the next hop. The device maintains only the route with the least metric value to a destination.

### Global Configuration

#### Default Metric

Specify the default metric value to be used for redistributed routes.

Metric is a property that contains a value used by a routing protocol to decide which route will be taken.

Default: 1

Acceptable Range: 1 to 16

#### Administrative Distance

Specify the administrative distance. It is a number used by the routers to find out the better route.

Default: 120

Acceptable Range: 1 to 255

#### RIP Version

Select the RIP version to be used for sending and receiving updates.

Available Options:

- Send V2 & Receive both
- V1
- V2

#### Timers

#### Update

Specify the time interval in seconds between two periodic routing updates.

Default: 30 seconds

Acceptable Range: 5 to 2147483647 seconds

#### Timeout

Specify the time in seconds after which the route becomes invalid.

Default: 180 seconds

Acceptable Range: 5 to 2147483647 seconds

#### **Garbage**

Specify the garbage time. It is amount of time that the device will advertise a route as being unreachable before deleting the route from the routing table.

Default: 120 seconds

Acceptable Range: 5 to 2147483647 seconds

#### **Default Information Originate**

Enable to control the distribution of the default route. It will generate and advertise a default route into the RIP-enabled networks.

The default setting is disabled.

#### **Redistribute Connected**

Click to enable the redistribution of connected routes into the RIP routing table.

Specify metric for redistributed connected routes.

Acceptable Range: 0 to 16

#### **Redistribute Static**

Click to enable the redistribution of static routes into the RIP routing table

Specify metric for redistributed static routes.

Acceptable Range: 0 to 16

#### **Redistribute OSPF**

Click to enable the redistribution of OSPF routes into the RIP routing table.

Specify metric for redistributed OSPF routes.

Acceptable Range: 0 to 16

#### **Redistribute BGP**

Click to enable the redistribution of BGP routes into RIP routing table.

Specify metric for redistributed BGP routes.

Acceptable Range: 0 to 16

Default Metric	<input type="text" value="1"/> (1-16)
Administrative Distance	<input type="text" value="120"/> (1-255)
RIP Version	<input checked="" type="radio"/> Send V2 & Recieve both <input type="radio"/> V1 <input type="radio"/> V2
<b>Timers</b>	
Update	<input type="text" value="30"/> (5-2147483647)
Timeout	<input type="text" value="180"/> (5-2147483647)
Garbage	<input type="text" value="120"/> (5-2147483647)
Default Information Originate	<input type="checkbox"/> on
Redistribute Connected	<input type="checkbox"/> Enable Metric <input type="text" value="0"/> (0-16)
Redistribute Static	<input type="checkbox"/> Enable Metric <input type="text" value="0"/> (0-16)
Redistribute OSPF	<input type="checkbox"/> Enable Metric <input type="text" value="0"/> (0-16)
Redistribute BGP	<input type="checkbox"/> Enable Metric <input type="text" value="0"/> (0-16)

**Figure 210: Global Configuration**

Click **Apply**.

#### RIP Networks

This section shows a list of available RIP networks including the corresponding netmasks.

#### Override Interface Configuration

You can manage interface configuration from this section.

#### Add RIP Network

1. Go to **Configure > Routing > RIP** and click **Add** in the **RIP Networks** section.
2. Enter the IPv4 address of the network and select a subnet mask from the dropdown list.

IPv4/Netmask *	<input type="text" value="192.168.1.1"/> / <input type="text" value="255.255.255.255"/> <input type="button" value="▼"/>
----------------	--

**Figure 211: Add RIP Network**

3. Click **Save**.

#### Override Interface Configuration

1. Go to **Configure > Routing > RIP** and click **Select Interface** under the **Override Interface Configuration** section.
2. Enter interface configuration details.

#### Interface

Select the interface for which you want to override the default configuration.

#### RIP Version

#### Send

Select the RIP version(s) to be used for sending the routing updates.

You can select V1 or V2 or both, V1 and V2. The selection overrides the version selected in the Global Configuration settings.

The default setting is **V2**.

### Receive

Select the RIP version to be used for receiving the routing updates.

You can select V1 or V2 or both, V1 and V2. The selection overrides the version selected in the Global Configuration settings.

The default setting is **V2 and V2**.

### Split Horizon

Enable to prevent the routing loops.

The default setting is disabled.

### Poisoned Reverse (*only applicable when Split Horizon is enabled*)

Enable to prevent the device from sending packets through the route that has become invalid.

The default setting is disabled.

### Authentication

Click to enable authentication of RIP packets.

If enabled, provide a password to authenticate the RIP packets.

### Passive Mode

Enable to prevent the interface from sending RIP advertisements.

The default setting is disabled.

Interface *	<input type="button" value="Select Here"/>
<b>RIP Version</b>	
Send	<input type="checkbox"/> V1 <input type="checkbox"/> V2
Receive	<input type="checkbox"/> V1 <input type="checkbox"/> V2
Split Horizon	<input checked="" type="checkbox"/> Enable
Poisoned Reverse	<input type="checkbox"/> Enable
Authentication	<input type="checkbox"/> Enable
Passive Mode	<input type="checkbox"/> Enable

**Figure 212: Override Interface Configuration**

3. Click Save.

## System Services

System Services allows configuration of device components along with the associated services.

Available configurations:

- *High Availability* - High Availability allows a second system to be used for redundancy or scalability.
- *Traffic Shaping Settings* - QoS traffic shaping allows network bandwidth to be limited or guaranteed.
- *RED* - Sophos RED allows seamless, encrypted, and tightly integrated connections between branch locations.
- *Log Settings* - Configure Syslog servers and enable/disable logs to be sent.
- *Data Anonymization* - Enable Data Anonymization and set Authorizers.
- *Traffic Shaping* - Displays list of predefined and custom policies and provides option to create a new traffic shaping policy.
- *Services* - View the current status and manage all the configured services.

## High Availability

Hardware failure such as a failure of the power supply, hard disk, or processor is the main reason behind the failure of a Internet security system and/or a device. To provide reliable and continuous connection to the Internet and to provide security services such as firewall, VPN, intrusion detection and prevention, virus scanning, web filtering, and spam filtering services, two devices can be configured to function as a single device and provide high availability.

Clustering technology is used to ensure high availability. In a cluster, devices are grouped together and instructed to work as a single entity.



**Note:** This feature is not available in models: CR15i, CR 15wi, CR25wi, CR35wi, CR15wiNG, CR25wiNG/6P and CR35wiNG/6P and on all WiFi models of XG Series devices.

### How a Cluster works

The device offers high availability by using virtual MAC address shared between a primary device and an auxiliary device linked together as a “cluster”.

Devices - primary and auxiliary device, are physically connected over a dedicated HA link port.

Typically, traffic enters your network by passing through a network switch. In an HA solution, one of the devices in the cluster has a virtual MAC address and traffic is forwarded to the cluster device which has the virtual MAC address. The device which has virtual MAC address is the primary device and the other peer is the auxiliary device. Primary device acts as a load balancer and forwards the traffic to the auxiliary device for processing. Auxiliary device can process traffic only if cluster is operating in the Active-Active mode.

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

Auxiliary device monitors the primary device through the dedicated HA link and if it does not receive any communication within the pre-configured time, the primary device is considered to have failed. In this case, the auxiliary device takes ownership of the virtual MAC address from the primary device, and becomes the primary device temporarily. Primary device automatically takes over from the auxiliary device once it starts functioning.

### HA terminology

#### 1. HA Cluster

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

#### 2. HA Configuration Modes

##### Active-Active

A configuration of HA cluster consists of a primary Device and an auxiliary device. In this mode, both primary device and auxiliary device process traffic while the primary unit is in charge of balancing the traffic. Decision of load balancing is taken by the primary device. The auxiliary device can take over only in case of a primary unit failure.

**Active-Passive**

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

**3. Primary Device**

The primary device also tracks the status of all cluster devices. In an Active-Active cluster, the primary device receives the entire network traffic and acts as load balancer to redirect traffic to the auxiliary device. In an Active-Passive cluster, the primary device processes the network traffic while the auxiliary device does not process any traffic but remains ready to take over if the primary device fails.

**4. Auxiliary Device**

Auxiliary device always waits to become the primary device.

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

**5. Dedicated HA Link Port**

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

**6. Load Balancing**

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

**7. Monitored Interface**

Set of interfaces that are selected to be monitored. Each device monitors its own selected interface(s) and if any of them goes down, the device removes itself from the cluster and a failover occurs.

**8. Virtual MAC**

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

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

**9. Primary State**

In Active-Active mode, the device that is in charge of receiving all the traffic and load balancing is said to be in “primary” state. A device can be in “primary” state only when the other device is in “auxiliary” state.

In Active-Passive mode, the device in charge of processing all the traffic is said to be in the “primary” state. A device can be in “primary” state only when the other device is in “auxiliary” state.

**10. Auxiliary State**

In Active-Active mode, the device that receives the traffic to be processed by it from the primary device is called to be in “auxiliary” state. A device can be in “auxiliary” state only when the other device is in “primary” state

In Active-Passive mode, the device which is not processing the traffic is called to be in “auxiliary” state. A device can be in “auxiliary” state only when the other device is in “primary” state.

**11. Standalone State**

A device is called to be in standalone state when it can still process network traffic and when the other device is not in position to process network traffic (i.e. in “fault” state or shut down).

**12. Fault State**

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

**13. Peer**

Once the HA cluster is configured, cluster devices are termed as peers i.e. for the primary device, the auxiliary device is its peer device and vice versa.

#### 14. Synchronization

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

#### 15. Device failover

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

#### 16. Link failover

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

#### 17. Session failover

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

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

### Configure HA

#### Points to be noted

- **WWAN, WLAN** - High Availability (HA) cluster cannot be configured if WWAN or WLAN is configured.
- **DHCP, PPPoE** - High Availability (HA) cluster cannot be configured in **Active-Active** mode if any of the interfaces are dynamically configured using DHCP or PPPoE protocols.
- You cannot configure interfaces using DHCP/PPPoE protocols when HA cluster is configured in **Active-Active** mode.
- **Masqueraded Connections** - In case of the manual synchronization events from any of the HA cluster devices, all the masqueraded connections will be dropped.
- HA can be disabled from either of the devices. If disabled from the primary device, HA will be disabled on both the devices. If disabled from the auxiliary device, HA will not be disabled on the primary device and will act as stand-alone device.
- After disabling HA, primary device IP schema will not change.
- After disabling HA, for the auxiliary device, all the ports except the dedicated HA link port and peer administration port will be disabled. The peer HA link IP will be the assigned IP address assigned to the dedicated HA link port while the peer administration IP will be the assigned IP address assigned to the peer administration port.
- If HA is disabled from a stand-alone machine, IP schema will not change.
- Super Administrator privileges are required to access the auxiliary device Admin console and therefore it can be accessed by “admin” user only and Live users/DHCP leases/IPsec live connections pages will not be displayed.
- After disabling HA, for the auxiliary device, for LAN zone all the administrative service – HTTPS, Telnet, SSH are allowed while for DMZ zone only HTTPS and SSH are allowed.
- For the auxiliary device, Deployment Wizard will not be accessible.
- Dedicated HA link port should be from any of the DMZ zone interface only. Make sure that the IP address of the HA link port of primary and auxiliary devices are in the same subnet.
- After enabling HA if backup without HA configuration is restored then HA will be disabled and the primary device will be accessible as per the backup configuration while auxiliary device will be accessible with the Auxiliary Admin IP Address.
- In **Active-Active** mode, mails will be quarantined separately on both the devices as SMTP proxy traffic is load balanced in round robin manner.

- In **Active-Passive** mode, mails will be quarantined on the primary device only.
- If quarantine digest is configured, both the devices in the cluster will send quarantine digests.
- Administrator can release quarantined mails of all the users from both the devices.
- User can release quarantined mails from the User Portal. The User Portal displays mails quarantined only on the primary device. Also, the user can release them from the quarantine digest mailed from the primary device.

**Note:**

- Not available in models CR15i, CR15wi, CR25wi, CR35wi, CR15wiNG, CR25wiNG/6P, CR25wiNG/6P and on all WiFi models of SG series devices.
- HA will get disabled if you run the Deployment Wizard.
- You must register the device to configure HA.

**Session failover**

- Session failover is possible for Forwarded TCP traffic under Route Mode, Bridge Mode, Mixed Mode and Multiport Bridge Mode.
- Session Failover is not possible for the following types of traffic under Route Mode, Bridge Mode, Mixed Mode and Multiport Bridge Mode:
  - Proxy Subsystem (Transparent/Direct/Parent proxy)
  - VPN Traffic
  - IPv4 and IPv6 forwarded traffic like UDP, ICMP, multicast, broadcast etc.
  - System generated traffic
  - AV Scanned sessions
  - Parent proxy traffic

**Load Balancing**

- Active-Active HA Cluster will successfully balance the load of following types of traffic under Route Mode, Bridge Mode, Mixed Mode and Multiport Bridge Mode:
  - TCP traffic passing through the proxy subsystem (Transparent/Direct/Parent)
  - Forwarded TCP Traffic
  - NATed (SNAT and Virtual Host) forwarded TCP traffic
  - HTTPS connection
  - VLAN traffic
- Active-Active HA Cluster **does not** load balance the following types of traffic under Route Mode, Bridge Mode, Mixed Mode and Multiport Bridge Mode:
  - VPN sessions
  - Traffic other than TCP (UDP, ICMP, multicast, broadcast etc.)
  - System generated traffic
  - Scanned FTP Traffic
  - Traffic coming through wireless RED devices and Access Points.
  - TCP Traffic for User Portal, Admin Console or Telnet Console
  - H323 Traffic sessions
  - Control traffic for all modules

**Before configuring HA**

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

- Both devices in the HA cluster i.e. primary and auxiliary device must be registered and have the same number of interfaces. Both member devices should be of the same model.
- Both devices in the HA cluster must have the same firmware version installed on it.
- **Active-Active:** Two separate licenses are required, one for the primary device and other for the auxiliary device. On both the devices, the same subscription modules should be enabled.
- **Active-Passive:** One license is required for the primary device. No license is needed for the auxiliary device.

- Cables to all the monitored ports on both the devices must be connected. Connect dedicated HA link port of both the devices with crossover cable.
- Dedicated HA link port should be from the DMZ zone interface only and must have a unique IP address on both the devices. SSH should be enabled for both the devices on the DMZ zone.
- WWAN and WLAN configuration must be disabled before HA configuration.
- DHCP/PPPoE configuration must be disabled before configuring HA in **Active-Active** mode.

### **Before enabling HA**

Before enabling HA, you need to provide the **Passphrase** and **Dedicated HA Link Port** details on the auxiliary device by selecting **Auxiliary** for **Initial HA Device State**. If the details are not configured on the auxiliary device then the primary device will not be able to connect to the auxiliary device.

### **Configure Primary Device**

1. Go to **Configure > System Services > High Availability**.
2. Enter High Availability details.

#### **Serial Number**

Displays serial number.

#### **Peer Serial Number**

Displays peer's serial number.

For the primary device, it displays the auxiliary device's serial number.

For the auxiliary device, it displays the primary device's serial number.

#### **HA Configuration Mode**

Select HA configuration mode for the cluster.

##### **Active-Active**

Select to configure a cluster for load balancing and failover HA. In Active-Active mode both, the primary device and the auxiliary device processes the traffic and monitors the status of the other cluster device. The primary device controls load balancing among both the cluster devices.

##### **Active-Passive**

Select to configure a cluster for failover HA. In Active-Passive mode the primary device processes all connections. The auxiliary device passively monitors the cluster status and remains synchronized with the primary device.

#### **Initial HA Device State**

Select to set initial device state from the available options.

##### **Available Options:**

Primary Auxiliary

#### **Passphrase**

**Passphrase** - Specify a passphrase for communication.

**Confirm Passphrase** - Confirm the specified passphrase.



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

#### **Dedicated HA Link Port**

Specify HA link port.

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

For example, if port E is configured as HA link port on the primary device then use port E only as HA link port on the auxiliary device. Make sure that the IP address of the HA link port for both, the primary device and auxiliary devices are in same subnet. Cluster devices use this link to communicate cluster information and to synchronize with each other.

Check [Before Configuring HA](#) before attempting to configure two devices as an HA pair.

#### Peer HA link IPv4

Specify the IP address configured on the HA link port of the peer device.

#### Peer Administration Port

Specify an administration port for the auxiliary device. This port can be used for administration purpose.

#### Peer Administration IP

Specify an administration IPv4/IPv6 address for the auxiliary device.

With this IP address, the Admin console of the auxiliary device can be accessed. Any user accessing the Admin console of the auxiliary device will be logged -in with an HA profile and have read-only rights.

#### Select Ports to be Monitored

Select the ports to be monitored.

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



**Note:** This feature is not supported in virtual security devices.

Serial Number	C118900001-959GBD
Peer Serial Number	-
HA Configuration Mode *	Active-Active
Initial HA Device State *	Primary
Passphrase *	Passphrase Confirm Passphrase
Dedicated HA Link Port *	
Peer HA Link IPv4 *	
Peer Administration Port *	PortA
Peer Administration IP *	IPv4
Select ports to be monitored	Add New Item

**Figure 213: Configure HA**

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

 **Note:** The device from which HA is enabled, acts as a Primary Device while the peer device acts as Auxiliary Device.

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

- Both devices will have the same configuration except the HA link port IP address.
- Additional options will be made available:

#### Primary Device

- Put on Standby (for Active-Passive mode)
- [Disable HA](#)
- Sync Auxiliary (used to synchronize auxiliary device and primary device configurations)

#### Auxiliary Device

- [Disable HA](#)
- Sync with Primary (used to synchronize auxiliary device and primary device configurations)

- By default, both the devices will synchronize automatically.
- As soon as Active-Active is configured, traffic load balancing is enabled. If required, it can be disabled from CLI console using the “system ha load-balancing on/off” command.

#### Disable HA

This page allows you to disable HA.

Go to **Configure > System Services > High Availability** and click **Disable HA**.

**Note:**

- HA can be disabled from either of the devices. If disabled from the primary device, HA will be disabled on both the devices. If disabled from the auxiliary device, HA will not be disabled on the primary device and will act as stand-alone device.
- After disabling HA, the primary device IP schema will not change.
- If HA is disabled from a stand-alone machine, the IP schema will not change.

After disabling HA, the auxiliary device will reboot, all the ports except the dedicated HA link port and peer administration port will be disabled. The dedicated HA link port will be assigned to the peer HA link IP address and the peer administration port will be assigned to the peer administration IP address.

**Switch Device to Standby Mode**

Standby mode for the device can be configured only if the cluster is operating in Active-Passive mode. The auxiliary device takes over as primary device.

**Synchronize HA Peers**

Under normal conditions, the auxiliary device is always synchronized with the primary device. However, if required, the auxiliary device can also be forcefully synchronized with the primary device.

Manual synchronization process can be initiated from either of the peers. If synchronized from the primary device, the primary device will push updates and if synchronized from the auxiliary device, the auxiliary device will pull the updates from the primary device.

Go to **Configure > System Services > High Availability** and click **Sync Auxiliary** to manually synchronize the auxiliary device with the primary device.

The matrix illustrates the HA state transitions from which synchronization is possible between HA peers. For example, synchronization is possible when the device in **Primary** state goes in **Fault** state but not when it goes in **Auxiliary** state.

From/To	Standalone	Primary	Auxiliary**	Fault
Standalone	No	Yes	Yes*	No
Primary	Yes	No	No	Yes
Auxiliary**	Yes	No	No	Yes
Fault	No	No	Yes	No

\*Possible when dedicated link goes down and comes back again

\*\*When device transits into Backup mode, it will soft boot

Manual synchronization gets the data and configuration updates except reports from the primary device.

**Services Support**

All the services except below listed services will not run on auxiliary device.

- Routing service
- VPN service
- Network service
- Logon server

**Traffic Shaping Settings**

This page allows you to configure default Traffic Shaping settings. All the bandwidth-related data are displayed only in KBps (1000 bytes per second).

The settings are as follows:

**Total Available WAN Bandwidth**

Specify maximum bandwidth limit in KBps. It is generally a sum of all WAN links' maximum limits.

Default: 100000 KBps

Acceptable Range (KBps): 1 to 2560000

### **Optimize for Real-Time (VoIP)**

Enable to give priority to real-time traffic like VOIP over all other traffic.

If disabled, priority will be applicable only for excess bandwidth i.e. bandwidth remaining after guaranteed bandwidth allocation.

### **Enforce Guaranteed Bandwidth**

The Administrator can enforce the handling of all internet-bound traffic by any Traffic Shaping Policy applied to it. If there is no policy applied to the traffic, it will be handled by the Default Policy.

Enable to enforce bandwidth restriction on the traffic to which the Traffic Shaping Policy is not applied.

Disable if you do not want to enforce bandwidth restriction on the traffic to which the Traffic Shaping Policy is not applied. It will only handle traffic on which the Traffic Shaping Policy is applied.

### **Default Policy**

The Default Policy will be applicable to the traffic which does not have any Traffic Shaping Policy applied.

#### **Guarantee**

Specify bandwidth which is the minimum guaranteed bandwidth that the user can use.

Default: 1 KBps

Acceptable Range (KBps): 1 to 2560000

#### **Limit**

Specify bandwidth which is the maximum bandwidth that the user can use, if available.

Default: 100000 KBps

Acceptable Range (KBps): 1 to 2560000

#### **Priority**

Set the bandwidth priority. Priority can be set from 1 (highest) to 7 (lowest) depending on the traffic required to be shaped.

#### **Available Options:**

1 – Business Critical  
2 – Normal  
6 – Bulky - FTP  
7 – Best Effort – e.g. P2P

### **Show Bandwidth Usage**

Click to view Bandwidth Usage.

Total Available WAN Bandwidth *	<input type="text" value="100000"/> KBps[1 - 2560000]
Optimize for Real-Time (VoIP) *	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
Enforce Guaranteed Bandwidth *	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
Default Policy *	Guarantee <input type="text" value="1"/> KBps[1 - 2560000] Limit <input type="text" value="100000"/> KBps[1 - 2560000] Priority <input type="text" value="7-[Best Effort - e.g P2P](Lowest)"/>

**Figure 214: Traffic Shaping Settings**

### Related information

[How to setup application filter](#)

## RED

This page describes how to enable RED.

RED is short for Remote Ethernet Device and is a means to connect remote sites, e.g., branch offices, to your main office as if the remote site was part of your local network.

The setup consists of the Sophos XG Firewall in your main office and a Remote Ethernet Device (RED) in your remote office. Establishing a connection between the two is utmost easy as the RED device itself does not need to be configured at all. As soon as the RED device is connected to your device it behaves like any other Ethernet device on your device. All traffic of your branch office is safely routed via your device which means that your branch office is as secure as your local network.

These types of RED devices are currently available:

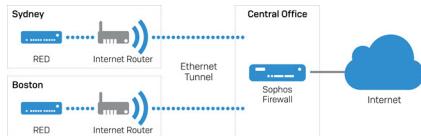
- RED 10: RED solution for small remote offices
- RED 15: RED solution for medium remote offices
- RED 15w: RED solution for small remote offices, including WiFi.
- RED 50: RED solution for bigger remote offices which comes with two uplink interfaces.

Additionally, you have the choice to establish a RED Site-to-Site tunnel between two SF devices which are connected through the RED technology on Layer 2. One device acts as server while the other is the client. For more information, see chapter [Configure RED Site-to-Site Tunnel](#).

Each RED device or SF device that is configured here is able to establish a connection to your SF device.

 **Note:** For RED devices to be able to connect, you need to enable RED support on the [Configure > System Services > RED](#) page first.

### RED setup example



### Related tasks

[Add RED](#) on page 119

This page allows you to configure a Remote Ethernet Device (RED) at a remote office.

### Configure RED

This page describes how to configure RED.

1. Go to [Configure > System Services > RED](#) and enable RED.
2. Specify the following:

**Organization Name**

Specify the name of the organization.

**City**

Specify the city where the organization is located.

**Country**

Select the country where the organization is located.

**Email**

Specify an email address.

The screenshot shows a configuration interface for enabling a Remote Ethernet Device (RED). At the top, there is a blue 'ON' toggle switch labeled 'RED Status'. Below it are four input fields: 'Organization Name \*' (empty), 'City \*' (empty), 'Country \*' (set to 'United Kingdom'), and 'Email \*' (empty). At the bottom is a blue 'Apply' button.

**Figure 215: Enable RED**

- Click **Apply**.



**Note:** If the message “Registering with RED service failed. Please make sure that this device can connect to the Internet on port 3400” appears, some kind of network problem is indicated. You should first check if you can reach `red.astaro.com` through port 3400 (via console command `telnet red.astaro.com 3400`). If so, the error might be due to a high network load. Retry to connect later.

The RED status is now activated. Sophos XG Firewall is now registered at the RED Provisioning Service (RPS) of Sophos to act as a RED hub. You can now continue by adding one or more RED devices at **System > Network > Interfaces**.

You can enable the **Automatic Device Deauthorization**.

**Related tasks**

[Add RED](#) on page 119

This page allows you to configure a Remote Ethernet Device (RED) at a remote office.

**Force TLS 1.2**

This page describes how to force TLS 1.2.

For security reasons it is recommended to force the RED device to use only TLS 1.2. This option is disabled by default to ensure that new RED devices can connect to the Firewall and first have a firmware upgrade to support TLS 1.2.



**Note:** If you want to add new RED devices, first disable TLS to ensure that the RED devices are able to connect to the Firewall.

- Ensure that RED is enabled.
- In the **Force TLS 1.2** area select **Enable**.
- Click **Apply**.

**Automatic Device Deauthorization**

This page describes how to deauthorize a RED device.

When RED is enabled, you can specify if disconnected RED devices should automatically be deauthorized after a certain time span. With this feature, you can prevent stolen RED devices from connecting to Sophos XG Firewall.



**Note:** The **Automatic Device Deauthorization** does not work for a RED tunnel between 2 Sophos XG Firewall devices.

1. Ensure that RED is activated.
2. Select **Enable** next to **Automatic Device Deauthorization**.
3. Enter a time span for **Deauthorize After**.
4. Click **Apply**.

Automatic Device Deauthorization will now be successfully configured.

When a RED device reconnects after being disconnected for a time span longer than the defined time span, it will automatically be disabled.

### Disable RED

This page describes how to disable RED.

Disabling RED will not cause the deletion of the REDs. If you disable the RED functionality, RED devices will be deactivated and lose their connection. If you re-enable the RED functionality, the REDs will be activated again.

1. Click the toggle switch of the **RED Status**.
2. Confirm deactivation by clicking on the **Confirm removal of RED configuration** button.

RED is now deactivated. All RED devices will be disconnected.

## Log Settings

Device provides extensive logging capabilities for traffic, system and network protection functions. Detailed log information and reports provide historical as well as current analysis of network activity to help identify security issues and reduce network abuse. To view logs, relevant modules must be subscribed.

Device can log many different network activities and traffic including:

- Firewall Rules log
- Anti Virus infection and blocking
- Web filtering, URL and HTTP content blocking
- Signature and anomaly attack and prevention
- Spam filtering
- Administrator logs
- User Authentication logs
- SSL VPN logs
- Web Server Protection logs
- Advanced Threat Protection logs
- Heartbeat logs

Device can either store logs locally or send logs to external syslog servers for storage and archival purposes. Traffic Discovery logs can be stored locally only.

Syslog is an industry standard protocol/method for collecting and forwarding Logs from devices to a server running a syslog daemon usually via UDP Port 514. Logging to a central syslog server helps in aggregation of logs and alerts.

If configured, device sends a detailed log to an external syslog server in addition to the standard event log. Device Syslog support requires an external server running a syslog daemon on any of the UDP Port. When configuring logging to a syslog server, one needs to configure the facility, severity and log file format. One can also specify logging location if multiple syslog servers are defined.

Device logs all activity and includes every connection source and destination IP Address (IPv4 / IPv6), IP service, and number of bytes transferred.

A Syslog service simply accepts messages, and store them in files or prints. This form of logging is the best as it provides a central logging facility and a protected long-term storage for logs. This is useful both in routine troubleshooting and in incident handling.

Use this page to configure below settings:

- Syslog Servers - Configure Syslog server for logs storage and archival purposes.
- Log Settings - Configure logs to be sent to the Syslog server.

## Syslog Servers

The Syslog Servers section displays list of configured syslog servers. You can sort the list based on server name. The page also provides option to add, update, or delete the server.

## Log Settings

After configuring syslog server, configure logs to be sent to the syslog server by selecting checkbox against the log under **Syslog**. If multiple syslog servers are configured, you can send various logs on different servers.

To record logs you must enable the respective log and specify logging location. Administrator can choose between On-Device (local) logging or Syslog logging. Administrator can also disable logging temporarily. Below are the different log types with their description:

### Firewall

Firewall Log records following events:

- Firewall Rules  
Log records the entire traffic for Firewall.
- Invalid Traffic  
Log records the dropped traffic that does not follow the protocol standards, invalid fragmented traffic and the traffic whose packets or device is not able to relate to any connection.
- Local ACLs  
Log records the entire (allowed and dropped) incoming traffic.
- DoS Attack  
The DoS Attack Log records attacks detected and prevented by the device i.e. dropped TCP, UDP and ICMP packets.

To generate logs, go to **System > System Services > DoS & Spoof Protection** and click **Apply Flag** against **SYN Flood, UDP Flood, TCP Flood, and ICMP/ICMPv6 Flood** individually.

- Dropped ICMP Redirected Packet  
Log records all the dropped ICMP redirect packets.  
To generate log, go to **System > System Services > DoS & Spoof Protection** and click **Apply Flag** against **Disable ICMP/ICMPv6 Redirect Packet**.
- Dropped Source Routed Packet  
Log records all the dropped source routed packets.

To generate log, go to **System > System Services > DoS & Spoof Protection** and click **Apply Flag** against **Drop Source Routed Packets**.

- Dropped Fragmented Traffic  
Log records the dropped fragmented traffic.
- MAC Filtering  
Log records the dropped packets when filtering is enabled from Spoof prevention.
- IP-MAC Pair Filtering

- Log records the dropped packets when filtering is enabled from Spoof prevention.
- IP Spoof Prevention
  - Log records the dropped packets when filtering is enabled from Spoof prevention.
- SSL VPN Tunnel
  - Log records of SSL VPN traffic.
- Protected Application Server
  - Log records of protected application server traffic.
- Heartbeat
  - Log records of Heartbeat traffic.
- ICMP Error Message
  - Log records of ICMP error messages such as network/host/port unreachable, destination network/host unknown and so on.

Policy Rules	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Invalid Traffic	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Local ACLs	<input checked="" type="checkbox"/>	<input type="checkbox"/>
DoS Attack	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Dropped ICMP Redirected Packet	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Dropped Source Routed Packet	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Dropped Fragmented Traffic	<input checked="" type="checkbox"/>	<input type="checkbox"/>
MAC Filtering	<input checked="" type="checkbox"/>	<input type="checkbox"/>
IP-MAC Pair Filtering	<input checked="" type="checkbox"/>	<input type="checkbox"/>
IP Spoof Prevention	<input checked="" type="checkbox"/>	<input type="checkbox"/>
SSL VPN Tunnel	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Protected Application Server	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Heartbeat	<input checked="" type="checkbox"/>	<input type="checkbox"/>

**Figure 216: Firewall Rule****IPS**

Records detected and dropped attacks based on unknown or suspicious patterns (anomaly) and signatures.

Anomaly	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Signatures	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

**Figure 217: IPS****Anti Virus**

Virus detected in HTTP, SMTP, FTP, POP3, IMAP4, HTTPS, SMTPS, IMAPS and POPS traffic.

HTTP	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
FTP	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
SMTP	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
POP3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
IMAP	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
HTTPS	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
SMTPS	<input checked="" type="checkbox"/>	<input type="checkbox"/>
POPS	<input checked="" type="checkbox"/>	<input type="checkbox"/>
IMAPS	<input checked="" type="checkbox"/>	<input type="checkbox"/>

**Figure 218: Anti-Virus****Anti Spam**

SMTP, POP3, IMAP4, SMTPS, POPS, IMAPS spam and probable spam mails.

SMTP	<input checked="" type="checkbox"/>	<input type="checkbox"/>
POP3	<input checked="" type="checkbox"/>	<input type="checkbox"/>
IMAP	<input checked="" type="checkbox"/>	<input type="checkbox"/>
SMTPS	<input checked="" type="checkbox"/>	<input type="checkbox"/>
POPS	<input checked="" type="checkbox"/>	<input type="checkbox"/>
IMAPS	<input checked="" type="checkbox"/>	<input type="checkbox"/>

**Figure 219: Anti-Spam****Content Filtering**

Web filtering and Application Filtering logs.

Log records of the name of applications/URLs accessed and their categories.

**Note:**

To view the logs:

- Web Filter and Application Filter Policies should be applied in Firewall Rule.
- **Log Firewall Traffic** under **Firewall** page should be enabled.

Web Filter	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Application Filter	<input checked="" type="checkbox"/>	<input type="checkbox"/>

**Figure 220: Content Filtering****Events**

Admin Events: Log records of configurations done through Admin Console.

Authentication Events: Log records of all authentication related events.

System Events: Log records of all system related events like Gateway Up/Down, Anti Virus updates etc.

Admin Events	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Authentication Events	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
System Events	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

**Figure 221: Events****Web Server Protection**

Web Server Protection Events.

-  **Note:** Web Server Protection logs are not available in CR10iNG, CR15i, CR15wi, CR15iNG, CR15wiNG, CR25ia, CR25wi, CR35ia and CR35wi Sophos Devices.

Web Server Protection Events	<input checked="" type="checkbox"/>	<input type="checkbox"/>
------------------------------	-------------------------------------	--------------------------

**Figure 222: Web Server Protection****Advanced Threat Protection**

ATP Events: Log records of drop or alert event.

ATP Events	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
------------	-------------------------------------	-------------------------------------

**Figure 223: Advanced Threat Protection****Wireless**

Access Points & SSID: Log records of the connected APs and SSID.

Access Points & SSID	<input type="checkbox"/>	<input type="checkbox"/>
----------------------	--------------------------	--------------------------

**Figure 224: Wireless****Heartbeat**

Endpoint Status: Log records of the health status of the endpoint.

Endpoint Status	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
-----------------	-------------------------------------	-------------------------------------

**Figure 225: Heartbeat****System Health**

Usage: Log records of CPU usage, memory usage, no. of live users, interface and disk partition information.

Usage	<input type="checkbox"/>	<input type="checkbox"/>
-------	--------------------------	--------------------------

**Figure 226: System Health****Sandstorm**

Sandstorm Event: Log records of all Sandstorm events.

Sandstorm Events	<input checked="" type="checkbox"/>
------------------	-------------------------------------

**Figure 227: Sandstorm****Add Syslog Server**

This page describes how to add a syslog server.

1. Go to **Configure > System Services > Log Settings** and click **Add** under the **Syslog Servers** section.
2. Enter server details.

#### Name

Enter a unique name for the syslog server.

#### IP Address / Domain

Specify the IP address (IPv4 / IPv6) or domain name of the syslog server. Logs from the device will be sent to the server.

#### Port

Specify the port number for communication with the syslog server. The device will send logs using the configured port.

#### Facility

Select syslog facility for logs to be sent to the syslog server.

Facility indicates to the syslog server the source of a log such as operating system, the process or an application. It is defined by the syslog protocol.

The device supports several syslog facilities for received log.

#### Available Options:DAEMON

Daemon logs (information of services running in device as daemon).

#### KERNEL

Kernel log

#### LOCAL0 - LOCAL7

Log level information.

#### USER

Logging based on users who are connected to the server.

#### Severity Level

Specify severity levels of logs.

Severity level is the severity of the log that has been generated.

The device logs all the messages at and above the logging severity level you select. For example, select **ERROR** to log all messages tagged as **ERROR**, as well as any messages tagged with **CRITICAL**, **ALERT** and **EMERGENCY** and select **DEBUG** to log all messages.

The device supports following severity levels:**EMERGENCY** - System is not usable**ALERT**

- Action must be taken immediately**CRITICAL** - Critical condition**ERROR** - Error

condition**WARNING** - Warning condition**NOTIFICATION** - Normal but significant

condition**INFORMATION** - Informational**DEBUG** - Debug level messages.

#### Format

The device produces logs in the specified format. The device currently produces logs in device standard format.

Name *	<input type="text" value="Enter Name"/>
IP Address / Domain *	<input type="text" value="Enter IP Address"/>
Port *	<input type="text" value="Enter Port"/>
Facility *	<input type="text" value="DAEMON"/>
Severity Level *	<input type="text" value="Emergency"/>
Format *	<input type="text" value="Device Standard Format"/>

**Figure 228: Add Syslog Server**

 **Note:** You can configure maximum five syslog servers.

3. Click Save.

Once you add the server, go to the **System > System Services > Log Settings** page and enable all those logs, which are to be sent to the syslog server in the section **Log Settings**.

## Data Anonymization

This page allows you to enable/disable data anonymization and select authorizer administrators, also to de-anonymize all the user identities - Username, IP Address, MAC Address and Email Address in all logs /activities / reports.

View the report from **Configure > System Services > Data Anonymization**.

Once Data Anonymization is enabled, the Device anonymizes all the user identities. It means user identities in all the logs and reports are displayed in encrypted form.

To view the actual details, IT Administrator has to de-anonymize the same. To de-anonymize, approval from one of the authorizers configured on the **Configure > System Services > Data Anonymization** page is required.

### Data Anonymization Setting

Enable data anonymization for the IT administrator to view or download user-specific activities, logs or reports. Apart from the IT administrator, at least one independent authorizer with the administrative privileges is required.

Once enabled:

1. All the user identities - username, IP address (IPv4 / IPv6), MAC address and email address in all logs /activities / reports are anonymized.
2. If an IT administrator wants to de-anonymize above mentioned user details, approval is required from at least one of the Authorizers.
3. Similarly, to disable data anonymization, approval from at least one of the Authorizers is required.

 **Note:** To enable/disable data anonymization if you are logged in as one of the Authorizers, approval from at least one of the other Authorizers is required.

This section provides the following options:

#### Enable Data Anonymization

Click to enable Data Anonymization.

#### Select Authorizer

- **Administrator List** displays all the administrators.

- Click the check-box given under Select Authorizer menu to select the administrator. All the selected administrators are displayed under **Selected Authorizer** list.

Enable Data Anonymization

Select Authorizer

admin	-
<a href="#">Add New Item</a>	

[Apply](#)

## Exceptions

This section allows to de-anonymize all the user identities - Username, IP Address, MAC Address and Email Address in all logs /activities / reports.

Depending on whether you want to de-anonymize the user identities in all logs /activities / reports or in particular log /activity / report, there are two ways to de-anonymize the user identities:

- From Data Anonymization page
- From Log Viewer page or Reports module

Follow the steps below to de-anonymize all the user identities - Username, IP Address, MAC Address and Email Address in all logs /activities / reports:

- Select Username(s) to be de-anonymized from user(s) listed under the User parameter.
- Specify IP Address(s) (IPv4 / IPv6) to be de-anonymized.
- If required, specify MAC Address(s) and Email Address(s) to be de-anonymized from Advanced Settings section.
- Click **Apply**. An Authorization Window shall pop-up. Given below are the parameters and their description:
  - User Name: Select the Authorizer configured from **Configure > System Services > Data Anonymization** page.
  - Password: Specify password for the selected Authorizer and click OK.
- Once approved, user identities in all logs and reports are decrypted and displayed with the actual user details.

**Exceptions**

<b>Users</b>	<div style="border-bottom: 1px solid #ccc; padding-bottom: 5px;"></div> <div style="text-align: right; padding-top: 5px;">Add New Item</div>
<b>IP</b>	<div style="border-bottom: 1px solid #ccc; padding-bottom: 5px;"></div> <div style="text-align: right; padding-top: 5px; position: relative;"> <span style="border: 1px solid #ccc; padding: 2px 10px; margin-right: 10px;">Search / Add</span> <span style="font-size: 2em; color: #ccc; font-weight: bold; position: absolute; right: -10px; top: 0;">+</span> </div>
<hr/>	
<b>Advanced Settings (MAC Address, Email)</b> <small>(?)</small>	
<b>MAC</b>	<div style="border-bottom: 1px solid #ccc; padding-bottom: 5px;"></div> <div style="text-align: right; padding-top: 5px; position: relative;"> <span style="border: 1px solid #ccc; padding: 2px 10px; margin-right: 10px;">Search / Add</span> <span style="font-size: 2em; color: #ccc; font-weight: bold; position: absolute; right: -10px; top: 0;">+</span> </div>
<b>Email</b>	<div style="border-bottom: 1px solid #ccc; padding-bottom: 5px;"></div> <div style="text-align: right; padding-top: 5px; position: relative;"> <span style="border: 1px solid #ccc; padding: 2px 10px; margin-right: 10px;">Search / Add</span> <span style="font-size: 2em; color: #ccc; font-weight: bold; position: absolute; right: -10px; top: 0;">+</span> </div>

**Apply**

**Figure 229: Exceptions**

#### From Log Viewer page or Reports module

Follow the steps below to de-anonymize a particular user identity in a particular log /activity / report:

1. To access the Log Viewer page, go to [Log Viewer](#). Else, you can view a report containing anonymized (encrypted) user identities from the Reports module.
2. Click the  icon against an anonymized (encrypted) string. A new window titled **De-Anonymize** shall pop up. Given below are the parameters and their description:
  - a. Anonymized String: Displayed the encrypted string. This is the string you want to decrypt.
  - b. De-Anonymized String: Displays the decrypted user identity i.e. actual user identity detail.



**Note:** This field is displayed blank until you specify password for the selected Authorised Username and click OK. Once approved, user identity in the log / report is decrypted and displayed with the actual user detail.

- c. Authorised Username: Displays the Authorizer list configured from **Configure > System Services > Data Anonymization** page. Select the desired Authorizer from the drop-down list.



**Note:** If you are logged in as one of the Authorizers, the drop-down list does not display your Username. Else, all the Authorizers are displayed.

d. Password: Specify password for the selected Authorizer.

e. De-Anonymize: Select the desired option:

- For this Search: Select to de-anonymize the user identity from the anonymized (encrypted) string selected in step 2, for this particular search only.
- Session: Select to de-anonymize the user identity from the anonymized (encrypted) string selected in step 2, until you log out of the Admin Console.
- Permanently: Select to permanently de-anonymize the user identity from the anonymized (encrypted) string selected in step 2.



**Note:** This is similar to the first method i.e. De-Anonymizing the user identities from the De-Anonymize page, where all the user identities in all logs and reports are decrypted and displayed with the actual user details.

f. Type: The drop-down list displays the type of user identity. Possible options are:

- Username
- IP Address
- MAC Address
- Email Address



**Note:** By default, it displays the user identity associated with the anonymized (encrypted) string, selected in step 2. For example, if the anonymized string is a Host, the type would be displayed as IP Address.

3. Click Save. The De-Anonymized String should now display the decrypted user identity i.e. actual user identity detail.
4. Click Cancel to close the **De-Anonymize** window. Now the selected log / report should display the decrypted user identity in place of the Anonymized String.

## Traffic Shaping

The **Traffic Shaping** tab displays a list of predefined and custom policies and provides the option to create a new traffic shaping policy, schedule traffic shaping policies, update parameters or delete policies.

You can also clone a policy. Select an existing policy and click the icon to create a copy of the selected policy. You can edit the cloned policy as per your requirements.

### Create New Traffic Shaping Policy

This page describes how to quickly configure a new traffic shaping policy. All the bandwidth-related data are displayed only in KBps (1000 bytes per second).

1. Go to **System > Profiles > Traffic Shaping** and click **Add**.
2. Specify the Traffic Shaping Policy details.

#### Name

Specify a unique name for the Policy.

#### Policy Association

Select an option to specify for whom the policy is to be created.

Available Options:**Users:** Restricts the bandwidth for a particular user or for a user group.**Rules:** Restricts the bandwidth of any entry to which the firewall rule is applied.**Web Categories:** Restricts the bandwidth for the URL categorized under the web categories.**Applications:** Restricts the bandwidth for the applications categorized under the application categories.

#### Rule Type

Select the type of policy.

Available Options:**Limit**: In this type of policy, the user cannot exceed the defined bandwidth limit.**Guarantee**: In this type of policy, the user is allocated the guaranteed amount of bandwidth and can draw the bandwidth up to the defined **Limit**, if available.

It enables to assign fixed minimum and maximum amounts of bandwidth to the users. By borrowing excess bandwidth when available, users are able to burst above guaranteed minimum limits, up to the defined **Limit**. Guaranteed rates also assure minimum bandwidth to critical users to receive constant levels of bandwidth during peak and non-peak traffic periods.

**Guarantee** represents the minimum guaranteed bandwidth and **Limit** represents the maximum bandwidth that the user can use, if available.

#### **Limit Upload/Download Separately**

Select from the available options.

Available Options:

**Disable**: Limits total (upload + download) bandwidth.

**Enable**: Limits upload and download bandwidth separately.

#### **Priority**

Set the bandwidth priority. Priority can be set from 0 (highest) to 7 (lowest) depending on the traffic required to be shaped.

0 - Real Time for example, VOIP 1 - Business Critical 2 to 5 - Normal 6 - Bulky - FTP 7 - Best Effort for Example, P2P

By default, priority is given to the real time traffic.

 **Note:** However, if you do not want this preference, the feature can be disabled from **Configure > System Services > Traffic Shaping Settings** page.

If **Optimize for Real-Time (VoIP)**, under **Configure > System Services > Traffic Shaping Settings** page is disabled the priority will be applicable only for excess bandwidth i.e. bandwidth remaining after guaranteed bandwidth allocation.

If **Optimize for Real-Time (VoIP)**, under **Configure > System Services > Traffic Shaping Settings** page is enabled the real-time traffic (Traffic Shaping policy with priority 0) like VOIP will be given precedence over all other traffic.

As priority is given to the real time traffic, it is possible that some non real-time traffic will not get their minimum guaranteed bandwidth. Specifically, if sum of **Limit** (max allowed) of all Traffic Shaping policies (real-time and non real-time) is greater than total max-limit then guaranteed bandwidth of the real-time policies will be fulfilled but non real-time might not get the minimum guaranteed bandwidth.

#### **Limit (in KBps) (only if Rule Type is Limit and Limit Upload/Download Separately is disabled)**

Specify the allowed total bandwidth.

Total bandwidth range: 2 – 2560000 KBps

Limit bandwidth should be greater than or equal to guaranteed bandwidth.

#### **Upload Bandwidth (in KBps) (only if Rule Type is Limit and Limit Upload/Download Separately is enabled)**

Specify the upload bandwidth.

Total bandwidth range: 2 – 2560000 KBps

#### **Download Bandwidth (in KBps) (only if Rule Type is Limit and Limit Upload/Download Separately is enabled)**

Specify the download bandwidth.

Total bandwidth range: 2 - 2560000 KBps

**Guarantee - Limit (in KBps) (only if Rule Type is Guarantee and Limit Upload/Download Separately is disabled)**

Specify the range for guaranteed bandwidth limit.

Total bandwidth range: 2 – 2560000 KBps

**Guarantee - Limit Upload (in KBps) (only if Rule Type is Guarantee and Limit Upload/Download Separately is enabled)**

Specify the range for guaranteed upload bandwidth.

Total bandwidth range: 2 – 2560000 KBps

**Guarantee - Limit Download (in KBps) (only if Rule Type is Guarantee and Limit Upload/Download Separately is enabled)**

Specify the range for guaranteed download bandwidth.

Total bandwidth range: 2 - 2560000 KBps

**Bandwidth Usage Type**

Select the type of bandwidth usage.

Available Options:**Individual:** Allocated bandwidth is for the particular User/Rule/Web Category/

Application only.**Shared:** Allocated bandwidth is shared among all the Users/Rules/Web

Categories/Applications who have been assigned this policy.

**Description**

Specify a description for the policy.

Name *	<input type="text"/>		
Policy Association	<input checked="" type="radio"/> Users	<input type="radio"/> Rules	<input type="radio"/> Web Categories
Rule Type	<input checked="" type="radio"/> Limit	<input type="radio"/> Guarantee	
Limit Upload/Download Separately	<input checked="" type="radio"/> Disable	<input type="radio"/> Enable	
Priority *	<input type="button" value="Select Priority"/>		
Limit *	<input type="text"/> KBps (2 - 2560000)		
Bandwidth Usage Type	<input checked="" type="radio"/> Individual	<input type="radio"/> Shared	
Description	<input type="text"/>		

**Figure 230: Add Traffic Shaping (QoS) Policy**

3. Click **Add** under **Add Schedule wise Traffic Shaping Policy Details to override default Traffic Shaping Policy Details** to Add Schedule wise Traffic Shaping Policy Details to override default Traffic Shaping Policy Details. Refer [Schedule Traffic Shaping Policy](#) for details.
4. Click **Save**.

**Schedule Traffic Shaping Policy**

This page describes how to schedule a traffic shaping policy. All the bandwidth-related data are displayed only in KBps (1000 bytes per second).

The page allows you to add a schedule-wise traffic shaping policy to override default traffic shaping policy details.

1. Go to **System > Profiles > Traffic Shaping**.

2. Click on the  icon of the requested policy.
3. Click **Add**.
4. Specify the Traffic Shaping Policy details.

#### **Name**

Displays the policy name.

#### **Rule Type**

Displays the default policy type set at the time of creation of policy. Modify if required.



**Note:** The configured policy type will override the default policy and will be applicable only for the selected scheduled time interval.

#### **Limit Upload/Download Separately**

Displays the default implementation strategy set at the time of creation of the policy. Modify if required.



**Note:** The configured policy type will override the default policy and will be applicable only for the selected scheduled time interval.

#### **Limit (in KBps) (only if Rule Type is Limit and Limit Upload/Download Separately is disabled)**

Displays the allocated total bandwidth. Modify if required.



**Note:** The modified bandwidth restriction is applicable only for the selected time interval.

#### **Upload Bandwidth (in KBps) (only if Rule Type is Limit and Limit Upload/Download Separately is enabled)**

Displays the allocated individual upload bandwidth. Modify if required.



**Note:** The modified bandwidth restriction is applicable only for the selected time interval.

#### **Download Bandwidth (in KBps) (only if Rule Type is Limit and Limit Upload/Download Separately is enabled)**

Displays the allocated individual download bandwidth. Modify if required.



**Note:** The modified bandwidth restriction is applicable only for the selected time interval.

#### **Guarantee - Limit (in KBps) (only if Rule Type is Guarantee and Limit Upload/Download Separately is disabled)**

Displays the range for the total guaranteed bandwidth. Modify if required.

Total bandwidth range: 2 – 2560000 KBps

#### **Guarantee - (only if Rule Type is Guarantee and Limit Upload/Download Separately is enabled)**

Displays the range for the guaranteed upload bandwidth. Modify if required.

Total bandwidth range: 2 – 2560000 KBps

#### **Guarantee - Limit Download (in KBps) (only if Rule Type is Guarantee and Limit Upload/Download Separately is enabled)**

Displays the range for the guaranteed download bandwidth. Modify if required.

Total bandwidth range: 2 - 2560000 KBps

#### **Schedule**

Select a schedule from the available list during which the traffic shaping policy will be applied.

Only recurring schedule can be applied.

If you are not sure about the schedule details, check [Schedule](#) to view the details.

Name *	128kbps link _Policy A
Rule Type	<input checked="" type="radio"/> Limit <input type="radio"/> Guarantee
Limit Upload/Download Separately	Disable
Limit *	
Schedule *	Select Schedule ▾

**Figure 231: Add Traffic Shaping (QoS) Policy Detail**

5. Click Save.

## Services

Services page allows you to view and manage the status of configured services.

You can view the current status and manage all the configured services:

- Anti-Spam
- Anti-Spam Center Connectivity
- Anti-Virus
- Authentication
- DNS Server
- IPS
- Web Proxy
- WAF
- DHCP Server
- DHCPv6 Server
- Router Advertisement Service
- Hotspot

### Parameters

#### Services

Name of the configured service.

#### Status

Current status of the service.

#### Manage

Click to start or stop or restart the respective service.

### Actions

#### Start

Start the service whose status is **Stopped**.

#### Stop Button

Stop the service whose status is **Running**.

#### Restart Button

Restart service: Only for authentication service and web proxy service.

**Status****No Web Server configured**

Indicates that no web server is configured.



**Note:** The **Start** button is disabled in this case.

**Connected**

Displayed when Internet connectivity is available for the gateway.

**Running**

Indicates that service has successfully started.

**Disconnected**

Displayed when Internet connectivity is unavailable for the gateway.

**Stopped**

Displayed when a service is stopped or when the respective subscription module is not subscribed.

Services	Status	Manage
Anti-Spam Anti-Spam Center Connectivity	Running Disconnected	<b>Stop</b>
Anti-Virus	Running	<b>Stop</b>
Authentication	Running	<b>Restart</b>
DNS Server	Running	<b>Stop</b>

**Figure 232: Services**

**Related concepts**

[Services](#) on page 170

This page allows you to configure authentication for firewall, VPN and admin traffic.

[IPS Policies](#) on page 374

This page displays the list of all the pre-defined and custom IPS policies.

[Authentication Policies](#) on page 494

The **Authentication Policies** menu allows you to configure policies for direct authentication.

[IPv6 Router Advertisement](#) on page 147

[Hotspots](#) on page 419

The **Hotspots** menu allows you to enable the Hotspots feature and define users who are allowed to view and distribute hotspot access information.

# Protect

---

## Firewall

---

Firewall rules are security rule-sets to implement control over users, applications or network objects in an organization. Using the firewall rule, you can create blanket or specialized traffic transit rules based on the requirement. This page provides centralized management for the entire set of device firewall rules. Sophos XG Firewall implements a single pane of management to secure all enterprise applications using configuration templates for various rule types.

Following sections provide more information on the Firewall section.

- [\*Introduction\*](#)
- [\*Managing Firewall Rules\*](#)
- [\*Default Firewall Rules\*](#)
- [\*Understanding Icons\*](#)
- [\*Understanding List of Firewall Rules\*](#)

### Introduction

Firewall rules are based on the following configurable templates:

1. [\*Business Application Rule\*](#)
2. [\*User/Network Rule\*](#)

### Managing Firewall Rules

You can see the entire list of added firewall rules from the **Firewall** page. Using the same page, you can update existing firewall rules or add new firewall rules. To change the processing order, you can re-order firewall rules by drag and drop action.



**Note:** All custom firewall rules can be re-ordered. The order of processing is top to bottom.

On the **Firewall** page, the following action buttons can be found.

- **IPv4:** Select to filter only IPv4 rules
- **IPv6:** Select to filter only IPv6 rules
- **Enable Filter:** Select to open filter view and apply the following filters for IPv4 or IPv6 rules:
  1. Rule Type - Select to filter rules based on Business, User or Network
  2. Source Zone - Select to filter rules based on LAN, WAN, DMZ, LOCAL, VPN or WiFi
  3. Destination Zone - Select to filter rules based on LAN, WAN, DMZ, LOCAL, VPN or WiFi
  4. State - Select to filter rules based on Unused, Disabled, Changed, New
  5. Rule ID - Specify Rule ID to see the specific rule.
- **Reset Filter** (Available if filter is enabled) - Select to reset all filters
- **Disable Filter** (Available if filter is enabled) - Select to close filter view
- **+ Add Firewall Rule** - Select to add a new rule among Business Application Rule, or User/Network Rule.

### Testing Firewall Rules

You can test and troubleshoot firewall rules using the policy tester. Click **Log Viewer** and then click the **Policy Test** tab.

## Default Firewall Rules

At the time of deployment, **Network Configuration Wizard** provides an option to enable User/Network Rule for LAN to WAN traffic and automatically creates default firewall rule **Default\_Network\_Policy**. You can apply Web filter, App filter and IPS policy through this default policy from the Wizard itself or from Web Admin console whenever required.

## Understanding Icons

There are various action icons as well as symbolic icons on the **Firewall** page. Color codes, meanings and associated actions of icons are shown below.

Icons	Meaning
	Business Application Rule Enabled
	Business Application Rule Disabled
	User Rule Disabled + Action - Accept
	User Rule Disabled + Action - Drop/Reject
	User Rule Enabled + Action - Drop/Reject
	User Rule Enabled
	Network Rule Enabled
	Network Rule Disabled + Action - Accept
	Network Rule Disabled + Action - Drop/Reject
	Network Rule Enabled + Action - Drop/Reject
	Anti-Virus Scanning Disable
	Anti-Virus Scanning Enable
	Application Control Disable
	Application Control Allow All
	Application Control Deny All
	Application Control Drop

Icons	Meaning
	Security Heartbeat Disable / No Restriction
	Security Heartbeat Enable - Green
	Security Heartbeat Enable - Yellow
	Security Heartbeat - No Restriction + No Heartbeat.
	Security Heartbeat - No Restriction + Green
	Security Heartbeat - No Restriction + Yellow
	Intrusion Prevention Disable
	Intrusion Prevention Enable
	NAT Disable
	NAT Enable
	Traffic Shaping Policy Disabled
	Traffic Shaping Policy Enabled
	Web Policy Disable
	Web Policy Allow
	Web Policy Deny
	Web Policy Drop
	Routing Enabled
	Routing Disabled
	Firewall Rule enabled. Click to disable the rule.
	Firewall Rule disabled. Click to enable the rule.
	Expand the rule for more information.
	Collapse Rule
	Edit Rule
	Delete Rule (not applicable for default rules)
	Dragger

Icons	Meaning
Color Codes	
Red	Reject/Drop
Green	Accept/Allow
Yellow	Drop (In case of policies)
Blue	On/Enable
Grey	Off/Disable

### Understanding the List of Firewall Rules

All added rules are available in the form of a list. Each rule in the list presents a quick snapshot of the rule.

#### Details of the rule:

- **Rule Name:** Name of the rule
- **In/Out:** Amount of traffic (in bytes) coming in or going out using the particular rule
- **Firewall Rule Features:** Status of schedule, Heartbeat, IPS, and traffic shaping
- **Source:** Source zone
- **Destination:** Destination zone
- **What:** Displays protected domains/services
- **Action:** Status of protected servers, status of web and application protection for user
- **ID:** Rule ID
- **User's Policy Applied:** Status of application filter, web policy, AV and AS scanning, NAT policy and route through gateway, if configured

To view details of the Source, Destination, What (type of service) and Features, hover over the Features.

Click  for the following options to appear:

- 
- 
- Clone Above
- Clone Below
- Add Above Network Rule
- Add Above Business Rule
- Add Below Network Rule
- Add Below Business Rule
- Add to Group: List of existing groups is displayed. You can edit the groups or create a new group.
- Delete
- Detach: To detach a firewall rule from a group.

### User / Network Rule

User/Network Rule is used to define access rights and protection to the network objects/hosts. In a nutshell, if you want to control traffic by source, service, destination, zone, then use a **Network Rule**. Additionally, the administrator has the option to attach user identity to a rule in order to customize access of assorted hosts/servers. Such an identity based rule is considered a **User Rule**.

You can view or add a User/Network Rule for IPv4 and IPv6 traffic.

1. [Add User / Network Rule \(IPv4\)](#)
2. [Add User / Network Rule \(IPv6\)](#)

### Add User/Network Rule (IPv4)

This page allows you to create firewall rules to control traffic that uses the IPv4 protocol. The firewall rules control traffic between internal and external networks and protect the network from unauthorized access. The device determines the rule to be applied based on the source and destination zone you configure in the firewall rule. Use this page to create identity-based firewall rules by applying them to users.

1. Go to **Protect > Firewall** and select **IPv4**. using the filter switch.
2. Click **+Add Firewall Rule** and **User/Network Rule**.
3. Enter the rule introduction details.

#### Rule Name

Enter a name for the rule.

#### Description

Enter a description for the rule.

#### Rule Position

Specify the position of the rule from the available options.

##### Available Options:

Top Bottom

#### Action

Specify an action for the rule traffic from the available options. **Accept** – Allow access**Drop** – Silently discard**Reject** – Deny access (“ICMP port unreachable” message is sent to the source)

When sending a response it might be possible that the response is sent using a different interface than the one on which the request was received. This may happen depending on the routing configuration done on the device.

For example: If the request is received on the LAN port using a spoofed IP address (public IP address or the IP address not in the LAN zone network) and no specific route is defined, the device will send a response to these hosts using the default route. Hence, the response will be sent through the WAN port.

Rule Name *	Description	Rule Position
<input type="text" value="Enter Rule Name"/>	<input type="text" value="Enter Description"/>	<input type="text" value="Bottom"/>
Action <input checked="" type="button" value="Accept"/> <input type="button" value="Drop"/> <input type="button" value="Reject"/>		

**Figure 233: About This Rule**

4. Enter the Source details.

#### Source Zones

Select the source zones allowed to the user.

A new zone can be created directly from this page itself or from **Configure > Network > Zones** page.

#### Source Networks and Devices

Select the source networks/devices allowed to the user.

A new network host can be created directly from this page itself or from **System > Hosts and Services**.

#### During Scheduled Time

Select the schedule allowed to the user.

A new schedule can be created directly from this page itself or from the **System > Profiles > Schedule** page.

Source Zones *	Source Networks and Devices *	During Scheduled Time
<input type="text"/>	<input type="text"/> Any	<input type="text"/> All the Time
<input type="button" value="Add New Item"/>	<input type="button" value="Add New Item"/>	

**Figure 234: Source**

- Enter the Destination and Services details.

#### Destination Zones

Select the destination zones allowed to the user.

#### Destination Networks

Select the destination networks allowed to the user.

A new network host can be created directly from this page itself or from **System > Hosts and Services**.

#### Services

Select the services allowed to the user.

A new service can be created directly from this page itself or from the **System > Hosts and Services > Services** page.

Destination Zones *	Destination Networks *	Services *
<input type="text"/>	<input type="text"/> Any	<input type="text"/> Any
<input type="button" value="Add New Item"/>	<input type="button" value="Add New Item"/>	<input type="button" value="Add New Item"/>

**Figure 235: Destination**

- Enter Identity details. Follow this step if you want to configure a User Rule.

#### Match known users

Select to enable a rule based on the user identity.

#### Show captive portal to unknown users (*available only if Match known users is selected*)

Select the check box to accept traffic from unknown users. Captive portal page is displayed to the user where the user can login to access the Internet.

Clear the check box to drop traffic from unknown users.

#### User or Groups(*available only if Match known users is selected*)

Select the user(s) or group(s) from the list of available options.

#### Exclude this user activity from data accounting. (*only available if Match known users is selected*)

Select to exclude user traffic activity from data accounting. In other words, the traffic allowed through this rule will not be accounted towards data transfer for the user.

By default, user's network traffic is considered in data accounting.

Match known users

Show captive portal to unknown users

User or Groups \*

Any

Add New Item

Exclude this user activity from data accounting

**Figure 236: Identity**

7. Enter Web Malware and Content Scanning details (*available only if Action selected for the traffic is Accept*).

#### Scan HTTP

Enable HTTP traffic scanning.

#### Decrypt & Scan HTTPS

Enable HTTPS traffic decryption and scanning.

#### Detect zero-day threats with Sandstorm

Send files downloaded using HTTP or HTTPS for analysis by Sandstorm. Sandstorm protects your network against unknown and unpublished threats (“zero-day” threats).

#### Scan FTP for Malware

Enable FTP traffic scanning.

8. Enter Advanced settings details (*available only if Action selected for the traffic is Accept*).

- a) Specify policies for User Applications.

#### Intrusion Prevention

Select an IPS policy for the rule. A new IPS policy can be created directly from this page itself or from **Protect > Intrusion Prevention > IPS Policies** page.

#### Traffic Shaping Policy

User’s traffic shaping policy will be applied automatically if **Match known users** is selected.

You need to select traffic shaping policy for the rule if **Match known users** is not selected.

#### Web Policy

Select a web policy for the rule.

A new web policy can be created directly from this page itself or from the **Protect > Web > Policies** page.

#### Apply Web Category based Traffic Shaping Policy

Click to restrict bandwidth for the URLs categorized under the Web category.

A three step configuration is required as follows:

1. Create a traffic shaping policy from the **System > Profiles > Traffic Shaping** page. Here, specify the **Policy Association** as **Web Categories**.
2. Now, on this page assign the created policy to **Web Policy**.
3. Select **Apply Web Category based Traffic Shaping Policy** to apply the rule.

#### Application Control

Select an application filter policy for the rule. A new application filter policy can be created directly from this page itself or from the **Protect > Applications > Application Filter** page.

#### Apply Application-based Traffic Shaping Policy

Click to restrict bandwidth for the applications categorized under the Application category.

A three step configuration is required as follows:

1. Create a traffic shaping policy from the **System > Profiles > Traffic Shaping** page. Here, specify the **Policy Association as Applications**.
2. Now, on this page assign the created policy to **Application Control**.
3. Select **Apply Application-based Traffic Shaping Policy** to apply the rule.

**User Applications**

**Intrusion Prevention** ⚠

None

**Traffic Shaping Policy**

User's policy applied

**Web Policy** ⚠

None

Apply Web Category based Traffic Shaping Policy

**Application Control** ⚠

None

Apply Application-based Traffic Shaping Policy

**Figure 237: User Applications**

- b) Configure Synchronized Security settings.

#### Minimum Source HB Permitted

Select a minimum health status that a source device must have to conform to this rule. Health status can be either **Green**, **Yellow** or **No Restriction**. If the health criterion is not met, access and privileges defined in this rule will not be granted to the user.

#### Block clients with no heartbeat

Heartbeat-capable devices can be required to send information on their health status in defined intervals - this is called a heartbeat.

Based on that information, you can restrict a source device's access to certain services and networks.

Enable/disable the option to require the sending of heartbeats.

#### Minimum Destination HB Permitted (*not available if the only Destination Zone selected is WAN*)

Select a minimum health status that a destination device must have to conform to this rule. Health status can be either **Green**, **Yellow** or **No Restriction**. If the health criterion is not met, access and privileges defined in this rule will not be granted to the user.



**Note:** You can use the option if you have selected multiple zones along with **WAN**.

#### Block request to destination with no heartbeat (*not available if the only Destination Zone selected is WAN*)

Heartbeat-capable devices can be required to send information on their health status in defined intervals - this is called a heartbeat.

Based on that information, you can block requests to destinations not sending heartbeat.

Enable/disable the option to require the sending of heartbeats.

 **Note:** You can use the option if you have selected multiple zones along with WAN.



**Synchronized Security** 

**Minimum Source HB Permitted:**

- GREEN
- YELLOW
- No Restriction

Block clients with no heartbeat

**Minimum Destination HB Permitted:**

- GREEN
- YELLOW
- No Restriction

Block request to destination with no heartbeat

**Figure 238: Synchronized Security**

- c) Enter NAT and Routing details.

#### Rewrite source address (Masquerading)

Select if you want to re-write the source address or specify a NAT policy.

Default: Disabled

#### Use Gateway Specific Default NAT Policy (*available only if Masquerading is selected*)

Select to override the default NAT policy with a gateway specific policy.

#### Override default NAT policy for specific Gateway (*available only if Use Gateway Specific Default NAT Policy is selected*)

Select to specify gateway and corresponding NAT policy. Multiple gateways and NAT policies can be added.

#### Use Outbound Address (*available only if Rewrite source address is selected*)

Select the NAT policy to be applied from the list of available NAT policies.

A new NAT policy can be created directly from this page itself or from the **System > Profiles > Network Address Translation** page.

Default: MASQ.

#### MASQ (Interface Default IP)

- IP Address of the Destination Zone as configured in **Configure > Network > Interfaces** will be displayed instead of (Interface Default IP) when single **Destination Zone** is selected.
- (Interface Default IP) will be displayed when multiple **Destination Zones** are selected.

#### Primary Gateway

Specify the Primary Gateway. This is applicable only if more than one gateway is defined.

 **Note:** On deletion of the gateway, **Primary Gateway** will display **WAN Link Load Balance** for WAN Destination Zone and **None** for other zones. In such case, firewall rule will not make routing decisions.

#### Backup Gateway

Specify the Backup Gateway. This is applicable only if more than one gateway is defined.

 **Note:** On deletion of the gateway, **Backup Gateway** will display **None**.

#### DSCP Marking

Select the DSCP Marking.

DSCP (DiffServ Code Point) classifies flow of packets as they enter the local network depending upon QoS. Flow is defined by 5 elements; source IP address, destination IP address, source port, destination port and the transport protocol.

For available options, refer to [DSCP Values](#).

**NAT & Routing**

Rewrite source address (Masquerading)

**Primary Gateway**

None

**Backup Gateway**

None

**DSCP Marking**

Select DSCP Marking

**Figure 239: NAT & Routing**

- Define logging option for the user application traffic.

#### Log Firewall Traffic

Select to enable logging of permitted and denied traffic.

Log Firewall Traffic

**Figure 240: Log Traffic**

- Click Save.

#### Add User / Network Rule (IPv6)

This page allows you to create firewall rules to control traffic that uses the IPv6 protocol. The firewall rules control traffic between internal and external networks and protect the network from unauthorized access. The device determines the rule to be applied based on the source and destination zone you configure in the firewall rule. Use this page to create identity-based firewall rules by applying them to users.

- Go to **Protect** > **Firewall** and select **IPv6**, using the filter switch.
- Click **+Add Firewall Rule** and **User/Network Rule**.
- Specify the policy introduction details.

#### Rule Name

Enter a name for the rule.

#### Description

Specify a description for the rule.

#### Rule Position

Specify the position of the rule from the available options.

#### Available Options:

Top Bottom

#### Action

Specify an action for the rule traffic from the available options. **Accept** – Allow access**Drop** – Silently discard**Reject** – Deny access (“ICMP port unreachable” message is sent to the source)

When sending a response it might be possible that the response is sent using a different interface than the one on which the request was received. This may happen depending on the routing configuration done on the device.

For example: If the request is received on the LAN port using a spoofed IP address (public IP address or the IP address not in the LAN zone network) and no specific route is defined, the device will send a response to these hosts using the default route. Hence, the response will be sent through the WAN port.

Rule Name *	Description	Rule Position
<input type="text" value="Enter Rule Name"/>	<input type="text" value="Enter Description"/>	Bottom
Action		
<input checked="" type="button" value="Accept"/>	<input type="button" value="Drop"/>	<input type="button" value="Reject"/>

**Figure 241: About This Rule**

#### 4. Specify Source details.

##### Source Zones

Select the source zones allowed to the user.

##### Source Networks and Devices

Select the source networks/devices allowed to the user.

A new network host can be created directly from this page itself by clicking **Create new** or from **System > Hosts and Services**.

##### During Scheduled Time

Select the schedule allowed to the user.

A new schedule can be created directly from this page itself or from the **System > Profiles > Schedule** page.

Source Zones *	Source Networks and Devices *	During Scheduled Time
<input type="text" value="Any"/>	<input type="text" value="Any"/>	All the Time
<input type="button" value="Add New Item"/>	<input type="button" value="Add New Item"/>	

**Figure 242: Source**

#### 5. Specify Destination and Services details.

##### Destination Zones

Select the destination zones allowed to the user.

##### Destination Networks

Select the destination networks allowed to the user.

A new network host can be created directly from this page itself by clicking **Create new** or from **System > Hosts and Services**.

##### Services

Select the services(s) allowed to the user.

A new service can be created directly from this page itself or from the **System > Hosts and Services > Services** page.

Destination Zones *	Destination Networks *	Services *
<input type="text"/>	<input type="text"/> Any	<input type="text"/> Any
<a href="#">Add New Item</a>	<a href="#">Add New Item</a>	<a href="#">Add New Item</a>

**Figure 243: Destination**

- Specify Identity details.

**Match known users**

Select to enable a rule based on the user identity.

**Show Captive Portal to unknown users**

Select the check box to accept traffic from unknown users. Captive portal page is displayed to the user where the user can login to access the Internet.

Clear the check box to drop traffic from unknown users.

**User or Groups(*available only if Match known users is selected*)**

Select the user(s) or group(s) from the list of available options.

**Exclude this user activity from data accounting (*only available if Match known users is selected*)**

Select to enable/disable user traffic activity from data accounting.

By default, user's network traffic is considered in data accounting. Select to exclude certain traffic user data accounting. The traffic allowed through this rule will not be accounted towards data transfer for the user.

<input checked="" type="checkbox"/> Match known users	User or Groups *
<input type="checkbox"/> Show captive portal to unknown users	<input type="text"/> Any
	<a href="#">Add New Item</a>
<input type="checkbox"/> Exclude this user activity from data accounting	

**Figure 244: Identity**

- Specify Web Malware and Content Scanning details. (*available only if Action for the traffic is Accept*)

**Scan HTTP**

Enable HTTP traffic scanning.

**Decrypt & Scan HTTPS**

Enable HTTPS traffic decryption and scanning.

**Detect zero-day threats with Sandstorm**

Send files downloaded using HTTP or HTTPS for analysis by Sandstorm. Sandstorm protects your network against unknown and unpublished threats ("zero-day" threats).

- Specify Advanced settings details (*available only if Action for the traffic is Accept*)

- Specify policies for user applications.

**Intrusion Prevention (IPS)**

Select an IPS policy for the rule. A new IPS policy can be created directly from this page itself or from **Protect > Intrusion Prevention > IPS Policies** page.

**Traffic Shaping Policy**

User's traffic shaping policy will be applied automatically if **Match known users** is selected.

You need to select traffic shaping policy for the rule if **Match known users** is not selected.

### Web Policy

Select a web policy for the rule.

A new web policy can be created directly from this page itself or from the **Protect > Web > Policies** page.

### Apply Web Category based Traffic Shaping Policy

Click to restrict bandwidth for the URLs categorized under the Web category.

A three step configuration is required as follows:

1. Create a traffic shaping policy on the **System > Profiles > Traffic Shaping** page. Here, specify the **Policy Association** as **Web Categories**.
2. Now, on this page assign the created policy to **Web Policy**.
3. Select **Apply Web Category based Traffic Shaping Policy** to apply the policy.

### Application Control

Select an application filter policy for the rule. A new application filter policy can be created directly from this page itself or from the **Protect > Applications > Application Filter** page.

### Apply Application-based Traffic Shaping Policy

Click to restrict bandwidth for the applications categorized under the Application category.

A three step configuration is required as follows:

1. Create a traffic shaping policy from the **System > Profiles > Traffic Shaping** page. Here, specify the **Policy Association** as **Applications**.
2. Now, on this page assign the created policy to **Application Control**.
3. Select **Apply Web based Traffic Shaping Policy** to apply the policy.

The screenshot shows the 'User Applications' configuration page with the following sections and settings:

- Intrusion Prevention**: Set to "None".
- Traffic Shaping Policy**: Set to "User's policy applied".
- Web Policy**: Set to "None".
- Checkboxes:**
  - Apply Web Category based Traffic Shaping Policy**
  - Apply Application-based Traffic Shaping Policy**
- Application Control**: Set to "None".

**Figure 245: User Applications**

- b) Specify Routing details.

### Rewrite source address (Masquerading)

Disable if you do not want to re-write the source address or specify a NAT policy.

Default - Enabled

#### **Use Gateway Specific Default NAT Policy (*only if Masquerading is selected*)**

Click to override the default NAT policy with a gateway specific policy.

#### **Override default NAT policy for specific Gateway (*only if Use Gateway Specific Default NAT Policy is selected*)**

Enable to specify gateway and corresponding NAT policy. Multiple gateways and NAT policies can be added.

#### **Use Outbound Address (*only if Rewrite source address is selected*)**

Select the NAT policy to be applied from the list of available NAT policies.

A new NAT policy can be created directly from this page itself or from the **System > Profiles > Network Address Translation** page.

Default: **MASQ**.

#### **MASQ (Interface Default IP)**

- IP Address of the Destination Zone as configured in **Configure > Network > Interfaces** will be displayed instead of (Interface Default IP) when single **Destination Zone** is selected.
- (Interface Default IP) will be displayed when multiple **Destination Zones** are selected.

#### **Primary Gateway**

Specify the primary gateway. This is applicable only if more than one gateway is defined.



**Note:** On deletion of the gateway, **Primary Gateway** will display **WAN Link Load Balance** for WAN Destination Zone and **None** for other zones. In such case, firewall rule will not make routing decisions.

#### **Backup Gateway**

Specify the backup gateway. This is applicable only if more than one gateway is defined.



**Note:** On deletion of the gateway, **Backup Gateway** will display **None**.

#### **DSCP Marking**

Select the DSCP Marking.

DSCP (DiffServ Code Point) classifies flow of packets as they enter the local network depending upon QoS. Flow is defined by 5 elements; Source IP Address, Destination IP Address, Source port, Destination port and the transport protocol.

For available options, refer to [DSCP Values](#).

**NAT & Routing**

Rewrite source address (Masquerading)

**Primary Gateway**  
None

**Backup Gateway**  
None

**DSCP Marking**  
Select DSCP Marking

**Figure 246: NAT & Routing**

- Define logging option for the user application traffic.

**Log Firewall Traffic**

Click to enable logging of permitted and denied traffic.

Log Firewall Traffic

**Figure 247: Log Traffic**

- Click Save.

**DSCP Value**

DiffServ Code Point (DSCP) uses the 6 bits, thereby giving  $2^6 = 64$  different values (0 to 63). describes the standard DSCP values. Remaining DSCP values can be customized as per the QoS requirement.

Decimal	DSCP	Description
0	Default	Best Effort
8	CS1	Class 1 (CS1)
10	AF11	Class 1, Gold (AF11)
12	AF12	Class 1, Silver (AF12)
14	AF13	Class 1, Bronze (AF13)
16	CS2	Class 2 (CS2)
18	AF21	Class 2, Gold (AF21)
20	AF22	Class 2, Silver (AF22)
22	AF23	Class 2, Bronze (AF23)
24	CS3	Class 3 (CS3)
26	AF31	Class 3, Gold (AF31)
28	AF32	Class 3, Silver (AF32)
30	AF33	Class 3, Bronze (AF33)
32	CS4	Class 4 (CS4)

Decimal	DSCP	Description
34	AF41	Class 4, Gold (AF41)
36	AF42	Class 4, Silver (AF42)
38	AF43	Class 4, Bronze (AF43)
40	CS5	Class 5 (CS5)
46	EF	Expedited Forwarding (EF)
48	CS6	Control (CS6)
56	CS7	Control (CS7)

## Business Application Rule

Business Application Rule is used to protect internally or publicly hosted business applications or servers like SalesForce, Sharepoint etc.

Using Business Application Rule, the administrator can configure protection of the http and non-http web servers from unauthorized access over the Internet. You can also control access of protected server or services through a Business Application Rule.

Several templates are available that cover protection configuration for a variety of different types of http and non-http web servers and application. A list of these application templates appear on the Business Application Rule page.

### Adding a Business Application Rule

Go to **Protect > Firewall** and select **IPv4**. using the filter switch. Now, click on **+Add Firewall Rule** and select **Business Application Rule**. You can then select the **Application Template** from the list of available templates.

The application template allows you to choose the rule which suits the configuration of the required business application. Once you select the template, you can see the configuration page with few fields pre-populated. The pre-populated values eliminate the need to manually specify the configuration for securing your business application, but you may customize the settings according to your network setup or other requirements.

1. **DNAT/Full NAT/Load Balancing rule** - It is used to protect Non-Web servers, like mail or other servers hosted inside the network (LAN or DMZ). Using this template, you can define access rights of such servers to users who require access over the WAN or Internet. Additionally, you can use the following Non-web application template:
2. **Email Server (SMTP)**: Email Server (SMTP) rule is used to protect mail servers which are hosted internally in a network and require protection.
3. **Email Clients (POP & IMAP)** - Email Clients (POP and IMAP) rule is used to protect mail servers which are hosted publicly (WAN) and require protection.



#### Note:

If you delete Email Clients rule, the Emails which are under process by this rule will be queued but will not be delivered.

We recommend to follow below given steps so that you do not lose all the emails processed by this rule:

1. Before deleting this rule, clone this rule by choosing **Clone Above** option and change the **Action** to **Drop**. This cloned rule will hold all the incoming emails.
2. Go to **Email > Mail Spool** and check if spool is empty.
3. Once the spool is empty, delete both the firewall rules.

### Application Protection Templates for common HTTP-based Applications

SF-OS offers several pre-configured templates to create a protection rule for commonly used HTTP-based applications. You can use a pre-configured template to create a rule for the web application that is close to your configuration, then modify it to fit your needs.

Pre-configured templates for common HTTP applications include:

1. [Web Server Protection \(WAF\)](#) - Web Server Protection is used to protect HTTP or generic web application servers hosted in the network. This template is essentially WAF implementation but with additional benefit of defining WAF objects, rules, exceptions from the same page.
2. [Exchange Autodiscover](#)
3. [Exchange Outlook Anywhere](#)
4. [Exchange General](#)
5. [Microsoft Lync](#)
6. [Microsoft Remote Desktop Gateway 2008 and R2](#)
7. [Microsoft Remote Desktop Web 2008 and R2](#)
8. [Microsoft Sharepoint 2010 and 2013](#)

### Add Web Server Protection (WAF) Rule

This page allows you to control HTTP traffic flowing to and from a web application. Use this page to create a Web Server Protection (WAF) rule for traffic that uses the IPv4 protocol.

1. Go to **Protect > Firewall** and make sure that **IPv4** is selected.
2. Click **+Add Firewall Rule** and **Business Application Rule**.
3. Enter the general rule details.

#### Application Template

Select **Web Server Protection (WAF)** to define an application filter policy for HTTP-based applications.

#### Rule Name

Enter a name for the rule.

#### Description

Enter a description for the rule.

#### Rule Position

Specify the position of the rule.

#### Available Options:

- Top
- Bottom

Application Template <input type="button" value="Select"/>	Description <input type="text" value="Description"/>	Rule Position <input type="button" value="Top"/>
Rule Name * <input type="text" value="Rule name"/>		

**Figure 248: About this Rule**

4. Enter the **Hosted Server** details.

#### Hosted Address

Select the interface of the hosted server to which the rule applies. It is the public IP address through which Internet users access the internal server/host.



**Note:** When a client establishes a connection and accesses the web server, the web server does not obtain the client's real IP address. The server obtains the address of the interface used by the Web Application Firewall (WAF) since the connection is made through the WAF. The client's real IP address is available in the HTTP header

#### Listening Port

Enter a port number on which the hosted web server can be reached externally over the Internet. Default is port 80 for plaintext communication (HTTP) and port 443 for encrypted communication (HTTPS).

#### HTTPS

Select to enable or disable scanning of HTTPS traffic.

#### **HTTPS Certificate (*available only if HTTPS is selected*)**

Select the HTTPS certificate to be used.

#### **Redirect HTTP (*available only if HTTPS is selected*)**

Select to redirect HTTP requests. Thus, users entering the URL without “https://” will be redirected automatically to the hosted server.



**Note:** An HTTP request requires a host header if **Redirect HTTP** is enabled.

#### **Domains**

Enter the FQDN of domains for which the web server is responsible. Wildcards are not allowed.

Examples:

- example.com
- www.example.com
- subdomain.example.com

(*If HTTPS is enabled*): Domains that are part of the selected HTTPS certificate are automatically available in the **Domains** box.

The screenshot shows a configuration window for a hosted server. On the left, there's a dropdown menu for 'Hosted Address \*' with 'Address' selected. Next to it is a 'Listening Port \*' field containing '80'. Below these are two checkboxes: 'HTTPS' (unchecked) and 'Redirect HTTP' (unchecked). To the right is a 'Domains \*' section with an empty list box and a 'Search / Add' button with a plus sign. The entire window has a light gray background and a white content area.

**Figure 249: Hosted Server**

5. Specify the **Protected Server(s)** details.

#### **Path-specific routing**

You can enable path-specific routing to define (a path) to which web servers incoming requests are forwarded.

You can define that all URLs with a specific path, for example, /products/, are sent to a specific web server. On the other hand you can allow more than one web server for a specific request but add rules how to distribute the requests among the servers. Additionally, you can define that each session is bound to one web server throughout its lifetime (sticky session). This may be necessary if you host an online shop and want to make sure that a user sticks to one server during the shopping session. You can also configure to send all requests to one web server and use the others only as a backup.

For each hosted web server, one default site path route (with path '/') is created automatically. The device automatically applies the site path routes in the most reasonable way: starting with the strictest, i.e., longest paths and ending with the default path route which is only used if no other more specific site path route matches the incoming request. The order of the site path route list is not relevant. If no route matches an incoming request, (in case the default route was deleted), the request will be denied.

#### **Add New Path (*available only if Path-specific routing is selected*)**

Click **Add Path** to define a new path.



**Note:** **Add New Path** will only be active after at least one web server and one hosted web server have been created.

### Web Server (*not available if Path-specific routing is selected*)

With this option, you select the web servers that are to be protected. Select a web server from **Web Server list**. The selected web server is displayed on the right side of the table under **Selected Web Server(s)**.

A new web server can be created on the **Protect > Web Server > Web Servers** page.

**Figure 250: Protected Server(s)**

- Specify Access Permission details (*not available if Path-specific routing is selected*).

#### Allowed Client Networks

Select or add the allowed networks that should be able to connect to the hosted web server.

#### Blocked Client Networks

Select or add the denied networks that should be blocked to your hosted web server.

#### Authentication

Select a web app authentication profile or click **Create new** to create a new authentication profile. You can also create an authentication profile from the **Protect > Web Server > Authentication Policies** page.

**Figure 251: Access Permission**

- Add path **Exceptions** for the web servers.

Click **Add New Exception** to specify a new exception.

**Figure 252: Exceptions**

- Specify Advanced settings.
  - Specify **Policies** for Business Applications.

#### Protection

Select an application protection policy for the server or create a new one. A new application protection policy can be created directly from this page or from the **Protect > Web Server > Protection Policies** page. You can also choose to have **None** application protection.

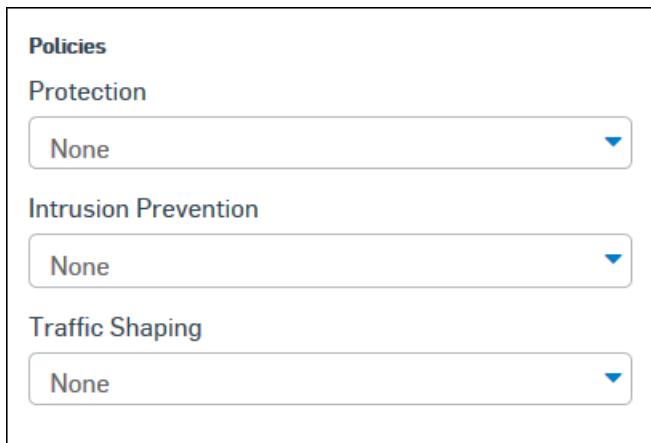
#### Intrusion Prevention

Select an Intrusion Prevention policy for the rule or create a new one. A new IPS policy can be created directly from this page or from the **Protect > Intrusion Prevention > IPS Policies** page. You can also choose to have **None** intrusion prevention.

### Traffic Shaping

The traffic shaping policy allocates & limits the maximum bandwidth usage of the user.

Select a traffic shaping policy for the rule or create a new one. A new traffic shaping policy can be created directly from this page or from the **System > System Services > Traffic Shaping** page. You can also choose to have **None** traffic shaping.



**Figure 253: Policies for Business Applications**

- Specify **Additional Options** for the added server.

### Disable Compression Support

By default, this check box is disabled and the content is sent compressed when the client requests compressed data. Compression increases transmission speed and reduces page load time. However, if websites are displayed incorrectly or users experience content-encoding errors when accessing your web servers, it may be necessary to disable compression. When the check box is enabled, the WAF will request uncompressed data from the web servers of this hosted web server and will send it uncompressed to the client, independent of the HTTP request's encoding parameter.

### Rewrite HTML

Select this option to have the device rewrite links of the returned webpages in order for the links to stay valid. Example: One of your web server instances has the hostname `yourcompany.local` but the hosted web server's hostname on the device is `yourcompany.com`. Thus, absolute links like `[a href="http://yourcompany.local/"]` will be broken if the link is not rewritten to `[a href="http://yourcompany.com/"]` before delivery to the client. However, you do not need to enable this option if either `yourcompany.com` is configured on your web server or if internal links on your webpages are always realized as relative links. It is recommended to use the option with Microsoft's Outlook web access and/or SharePoint portal server.



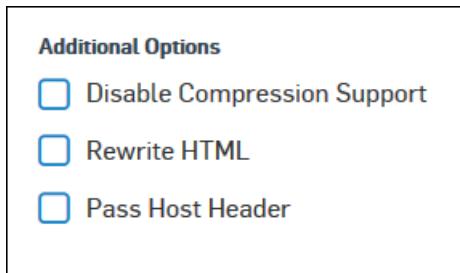
**Note:** HTML rewriting affects all files with a HTTP content type of `text/*` or `*xml*`, where `*` is a wildcard. Make sure that other file types, e.g. binary files, have the correct HTTP content type, otherwise they may get corrupted by the HTML rewriting process.

### Rewrite cookies (*available only if Rewrite HTML is selected*)

Select this option to have the device rewrite cookies of the returned web pages.

### Pass Host Header

When you select this option, the host header as requested by the client will be preserved and forwarded along with the web request to the web server. Whether passing the host header is necessary in your environment depends on the configuration of your web server.



**Figure 254: Advanced**

**9. Click Save.**



**Note:** As soon as a new HTTP based rule configuration has been created and saved or an existing HTTP based rule configuration has been altered and saved, all HTTP based business rules will be restarted. Any underlying client connection using a HTTP based business rule will get lost and has to be re-established.

The business application rule has been created and appears on the **Firewall** page when the **IPv4** filter is set.

**Related tasks**

[Add Path](#) on page 352

(only available for the HTTP based business application rules) This page describes how to define a path to which real web servers incoming requests are forwarded.

[Add Authentication Policy](#) on page 494

This page describes how to add a web app authentication policy.

[Add Exception](#) on page 353

(only available for the HTTP based business application rules) This page describes how to specify path exceptions for the web servers.

**Add Rule for Exchange Autodiscover**

(Only available for IPv4 policy) This page describes how to configure a rule for Exchange Autodiscover.

1. Go to **Protect > Firewall** and select **IPv4**, using the filter switch.
2. Click **+Add Firewall Rule** and **Business Application Rule**.
3. Specify the general rule details.

**Application Template**

Select **Exchange Autodiscover** to configure a policy for an Exchange Autodiscover environment.

**Description**

Enter a description for the rule.

**Rule Position**

Specify the position of the rule.

**Available Options:**

- Top
- Bottom

**Rule Name**

Specify a name for the rule.

Application Template	Description	Rule Position
Exchange Autodiscover	Description	Top
Rule Name *		
Rule name		

**Figure 255: About This Rule**

#### 4. Specify Hosted Server details.

##### Hosted Address

Specify the address of the hosted server to which the rule applies. It is the public IP address through which Internet users access an internal server/host.



**Note:** When a client establishes a connection and accesses the web server, the web server does not obtain the client's real IP address. The server obtains the address of the interface used by the Web Application Firewall (WAF) since the connection is made through the WAF. The client's real IP address is available in the HTTP header

##### Listening Port

Enter a port number on which the hosted web server can be reached externally over the Internet. Default is port 80 for plaintext communication (HTTP) and port 443 for encrypted communication (HTTPS).

##### HTTPS

Select this option to enable or disable HTTPS traffic.

##### HTTPS Certificate (*available only if HTTPS is selected*)

Select the HTTPS certificate to be used.

##### Redirect HTTP (*available only if HTTPS is selected*)

Select this option to redirect HTTP requests.

##### Domains

Use FQDN when you enter the domains the web server is responsible for, for example, shop.example.com.

The screenshot shows a configuration form for a hosted server. On the left, there is a dropdown menu labeled "Address". Below it are two checkboxes: "HTTPS" (unchecked) and "Redirect HTTP" (unchecked). On the right, there is a field labeled "Listening Port \*" with the value "80". Below that is a section labeled "Domains \*" with a "Search / Add" button and a plus sign (+).

**Figure 256: Hosted Server**

#### 5. Specify Protected Server(s) details.

##### Path-specific routing

You can enable path-specific routing to define (the path) to which web servers incoming requests are forwarded.

You can define that all URLs with a specific path, for example, /products/, are sent to a specific web server. On the other hand you can allow more than one web server for a specific request but add rules how to distribute the requests among the servers. Additionally, you can define that each session is bound to one web server throughout its lifetime (sticky session). This may be necessary if you host an online shop and want to make sure that a user sticks to one server during the shopping session. You can also configure to send all requests to one web server and use the others only as a backup.

For each hosted web server, one default site path route (with path /) is created automatically. The device automatically applies the site path routes in the most reasonable way: starting with the strictest, i.e., longest paths and ending with the default path route which is only used if no other more specific site path route matches the incoming request. The order of the site path route list is

not relevant. If no route matches an incoming request, (in case the default route was deleted), the request will be denied.

Default: Enabled

#### Add New Path (*available only if Path-specific routing is selected*)

Click **Add New Path** to define a new path.

[Add Path](#)

 **Note:** **Add New Path** will only be active only after at least one web server and one hosted web server have been created.

Default: /autodiscover, /Autodiscover, /AutoDiscover

#### Web Server (*not available if Path-specific routing is selected*)

Web servers are the application servers to be protected. Select a web server from the list of web servers or enter a web server and click **Create** to add a web server.

A new web server can be created directly from this page or from the **Protect > Web Server > Web Servers** page.



Path	Web Servers	Authentication	Allowed Client Networks	Blocked Client Networks	Sticky Sessions	Hot Standby	Edit/Delete
/autodiscover	0 Server(s)	Basic with passthrough	Any IPv4	N/A	x	x	
/Autodiscover	0 Server(s)	Basic with passthrough	Any IPv4	N/A	x	x	
/AutoDiscover	0 Server(s)	Basic with passthrough	Any IPv4	N/A	x	x	

[Add New Path](#)

**Figure 257: Protected Server(s)**

- Specify **Access Permission** details (*not available if Path-specific routing is selected*).

#### Allowed Client Networks

Select the allowed host(s)/network(s).

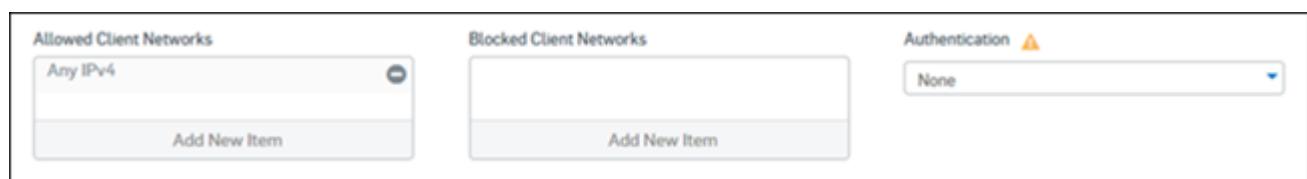
#### Blocked Client Networks

Select the blocked host(s)/network(s).

#### Authentication

Select the web application authentication profile from the list of available profiles.

You can also create a new authentication profile on this page or on the **Protect > Web Server > Authentication Policies** page.



Allowed Client Networks Any IPv4 <a href="#">Add New Item</a>	Blocked Client Networks <a href="#">Add New Item</a>	Authentication None <a href="#">None</a>
---	---	--

**Figure 258: Access Permission**

- Add path **Exceptions** for the web servers.

Click **Add New Exception** to specify new exception.

### [Add Exception](#)

Default: /autodiscover/\*,/Autodiscover/\*

Path	Client Resource	Checks	Categories	Status	Edit/Delete
/autodiscover/*,/Autodiscover/*	N/A	1	0	<input checked="" type="checkbox"/>	
<a href="#">Add New Exception</a>					

**Figure 259: Exceptions**

8. Specify Advanced settings.
- a) Specify **Policies** for Business Applications.

#### Protection

Select an application protection policy for the server or create a new one. A new application protection policy can be created directly from this page or from the **Protect > Web Server > Protection Policies** page. You can also choose to have **None** application protection.

#### Intrusion Prevention

Select an Intrusion Prevention policy for the rule or create a new one. A new IPS policy can be created directly from this page or from the **Protect > Intrusion Prevention > IPS Policies** page. You can also choose to have **None** intrusion prevention.

#### Traffic Shaping

The traffic shaping policy allocates & limits the maximum bandwidth usage of the user.

Select a traffic shaping policy for the rule or create a new one. A new traffic shaping policy can be created directly from this page or from the **System > System Services > Traffic Shaping** page. You can also choose to have **None** traffic shaping.

The screenshot shows a configuration panel titled 'Policies'. It contains three sections with dropdown menus: 'Protection' (set to 'None'), 'Intrusion Prevention' (set to 'None'), and 'Traffic Shaping' (set to 'None').

**Figure 260: Policies for Business Applications**

- b) Specify **Additional Options** for the added server.

#### Disable Compression Support

By default, this check box is disabled and the content is sent compressed when the client requests compressed data. Compression increases transmission speed and reduces page load time. However, if websites are displayed incorrectly or users experience content-encoding errors when accessing your web servers, it may be necessary to disable compression. When the check box is enabled, the WAF will request uncompressed data from the web servers of this hosted web server and will send it uncompressed to the client, independent of the HTTP request's encoding parameter.

#### Rewrite HTML

Select this option to have the device rewrite links of the returned webpages in order for the links to stay valid. Example: One of your web server instances has the hostname `yourcompany.local` but

the hosted web server's hostname on the device is yourcompany.com. Thus, absolute links like [a href="http://yourcompany.local/] will be broken if the link is not rewritten to [a href="http://yourcompany.com/"] before delivery to the client. However, you do not need to enable this option if either yourcompany.com is configured on your web server or if internal links on your webpages are always realized as relative links. It is recommended to use the option with Microsoft's Outlook web access and/or SharePoint portal server.



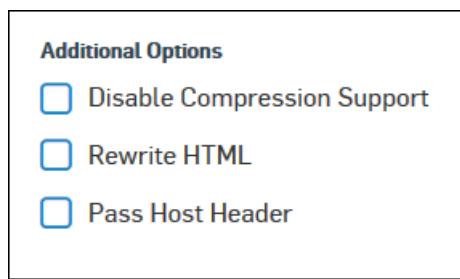
**Note:** HTML rewriting affects all files with a HTTP content type of text/\* or \*xml\*, where \* is a wildcard. Make sure that other file types, e.g. binary files, have the correct HTTP content type, otherwise they may get corrupted by the HTML rewriting process.

#### Rewrite cookies (*available only if Rewrite HTML is selected*)

Select this option to have the device rewrite cookies of the returned web pages.

#### Pass Host Header

When you select this option, the host header as requested by the client will be preserved and forwarded along with the web request to the web server. Whether passing the host header is necessary in your environment depends on the configuration of your web server.



**Figure 261: Advanced**

#### 9. Click Save.



**Note:** As soon as a new HTTP based policy configuration has been created and saved or an existing HTTP based rule configuration has been altered and saved, all HTTP based business rules will be restarted. Any underlying client connection using a HTTP based business rule will get lost and has to be re-established.

The firewall rule for Microsoft Remote Desktop Gateway 2008 and R2 has been created and appears on the **Firewall** page when the **IPv4** filter is set.

#### Add Rule for Exchange Outlook Anywhere

(only available for IPv4 policy) This page describes how to configure a rule for Exchange Outlook Anywhere.

1. Go to **Protect > Firewall** and select **IPv4**. using the filter switch.
2. Click **+Add Firewall Rule and Business Application Rule**.
3. Specify the general policy details.

#### Application Template

Select **Exchange Outlook Anywhere** to configure rule for Exchange Outlook Anywhere.

#### Description

Enter a description for the rule.

#### Rule Position

Specify the position of the rule.

**Available Options:** TopBottom

#### Rule Name

Specify a name for the rule.

The screenshot shows a configuration interface for a rule. At the top left is a dropdown menu labeled 'Application Template' with 'Exchange Outlook Anywhere' selected. To its right is a 'Description' field containing the placeholder 'Description'. Further right is a 'Rule Position' dropdown set to 'Top'. Below these are two input fields: 'Rule Name \*' with 'Rule name' typed in, and an empty 'Description' field.

**Figure 262: About This Rule**

- Specify Hosted Server details.

#### Hosted Address

Specify the address of the hosted server to which the rule applies. It is the public IP address through which Internet users access an internal server/host.



**Note:** When a client establishes a connection and accesses the web server, the web server does not obtain the client's real IP address. The server obtains the address of the interface used by the Web Application Firewall (WAF) since the connection is made through the WAF. The client's real IP address is available in the HTTP header

#### Listening Port

Enter a port number on which the hosted web server can be reached externally over the Internet. Default is port 80 for plaintext communication (HTTP) and port 443 for encrypted communication (HTTPS).

#### HTTPS

Select to enable or disable of HTTPS traffic.

#### HTTPS Certificate (*available only if HTTPS is selected*)

Select the HTTPS certificate to be used.

#### Redirect HTTP (*available only if HTTPS is selected*)

Select to redirect HTTP requests.

#### Domains

Use FQDN when you enter the domains the web server is responsible for, for example, shop.example.com.

The screenshot shows a configuration interface for a hosted server. On the left is a 'Hosted Address \*' field with a dropdown menu showing 'Address'. Next to it is a 'Listening Port \*' field with the value '80'. Below these are two checkboxes: 'HTTPS' (unchecked) and 'Redirect HTTP' (unchecked). On the right is a 'Domains \*' field with a 'Search / Add' button and a '+' icon.

**Figure 263: Hosted Server**

- Specify Protected Server(s) details.

#### Path-specific routing

You can enable path-specific routing to define (path) to which web servers incoming requests are forwarded.

You can define that all URLs with a specific path, for example, /products/, are sent to a specific web server. On the other hand you can allow more than one web server for a specific request but add rules how to distribute the requests among the servers. Additionally, you can define that each session is bound to one web server throughout its lifetime (sticky session). This may be necessary if you host an online shop and want to make sure that a user sticks to one server during the shopping

session. You can also configure to send all requests to one web server and use the others only as a backup.

For each hosted web server, one default site path route (with path '/') is created automatically. The device automatically applies the site path routes in the most reasonable way: starting with the strictest, i.e., longest paths and ending with the default path route which is only used if no other more specific site path route matches the incoming request. The order of the site path route list is not relevant. If no route matches an incoming request, (in case the default route was deleted), the request will be denied.

#### Add New Path (*available only if Path-specific routing is selected*)

Click **Add New Path** to define a new path.

[Add Path](#)

 **Note:** **Add New Path** will only be active after at least one web server and one hosted web server have been created.

Default: /rpc, /RPC

#### Web Server (*not available if Path-specific routing is selected*)

Web servers are the application servers that are to be protected. Select a web server from the list of web servers or click **Add New Item** to add a web server.

A new web server can be created directly from this page or from the **Protect > Web Server > Web Servers** page.



Path	Web Servers	Authentication	Allowed Client Networks	Blocked Client Networks	Sticky Sessions	Hot Standby	Edit/Delete
/rpc	0 Server(s)	Basic with passthrough	Any IPv4	N/A	*	*	
/RPC	0 Server(s)	Basic with passthrough	Any IPv4	N/A	*	*	

[Add New Path](#)

**Figure 264: Protected Server(s)**

- Specify Access Permission details. (*not available if Path-specific routing is selected*).

#### Allowed Client Networks

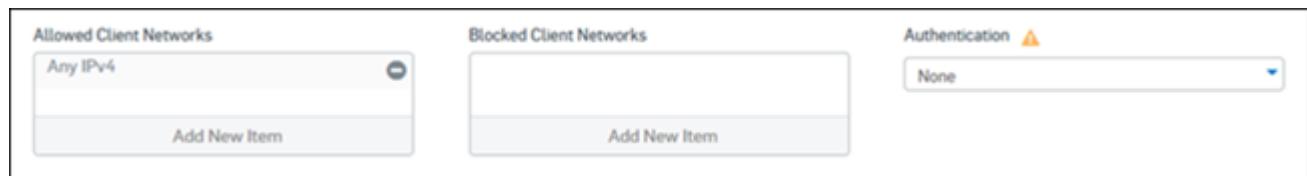
Select the allowed host(s)/network(s).

#### Blocked Client Networks

Select the blocked host(s)/network(s).

#### Authentication

Select the web application authentication profile from the list of available profiles. You can also create a new authentication profile from this page or from the **Protect > Web Server > Authentication Policies** page.



Allowed Client Networks	Blocked Client Networks	Authentication 
Any IPv4		None
<a href="#">Add New Item</a>	<a href="#">Add New Item</a>	

**Figure 265: Access Permission**

- Add path **Exceptions** for the web servers.

Click **Add New Exception** to specify new exception.

[Add Exception](#)

Default: /rpc/\*,/RPC/\*.

Path	Client Resource	Checks	Categories	Status	Edit/Delete
/rpc/*,/RPC/*	N/A	1	0	<input checked="" type="checkbox"/>	

[Add New Exception](#)

**Figure 266: Exceptions**

- Specify Advanced settings.

- Specify **Policies** for Business Applications.

#### Protection

Select an application protection policy for the server or create a new one. A new application protection policy can be created directly from this page or from the **Protect > Web Server > Protection Policies** page. You can also choose to have **None** application protection.

#### Intrusion Prevention

Select an Intrusion Prevention policy for the rule or create a new one. A new IPS policy can be created directly from this page or from the **Protect > Intrusion Prevention > IPS Policies** page. You can also choose to have **None** intrusion prevention.

#### Traffic Shaping

The traffic shaping policy allocates & limits the maximum bandwidth usage of the user.

Select a traffic shaping policy for the rule or create a new one. A new traffic shaping policy can be created directly from this page or from the **System > System Services > Traffic Shaping** page. You can also choose to have **None** traffic shaping.

Policies
Protection
None
Intrusion Prevention
None
Traffic Shaping
None

**Figure 267: Policies for Business Applications**

- Specify **Additional Options** for the added server.

#### Disable Compression Support

By default, this check box is disabled and the content is sent compressed when the client requests compressed data. Compression increases transmission speed and reduces page load time. However, if websites are displayed incorrectly or users experience content-encoding errors when accessing your web servers, it may be necessary to disable compression. When the check box is enabled, the WAF will request uncompressed data from the web servers of this hosted web server and will send it uncompressed to the client, independent of the HTTP request's encoding parameter.

## Rewrite HTML

Select this option to have the device rewrite links of the returned webpages in order for the links to stay valid. Example: One of your web server instances has the hostname `yourcompany.local` but the hosted web server's hostname on the device is `yourcompany.com`. Thus, absolute links like `[a href="http://yourcompany.local/"]` will be broken if the link is not rewritten to `[a href="http://yourcompany.com/"]` before delivery to the client. However, you do not need to enable this option if either `yourcompany.com` is configured on your web server or if internal links on your webpages are always realized as relative links. It is recommended to use the option with Microsoft's Outlook web access and/or SharePoint portal server.



**Note:** HTML rewriting affects all files with a HTTP content type of `text/*` or `*xml*`, where `*` is a wildcard. Make sure that other file types, e.g. binary files, have the correct HTTP content type, otherwise they may get corrupted by the HTML rewriting process.

## Rewrite cookies (*available only if Rewrite HTML is selected*)

Select this option to have the device rewrite cookies of the returned web pages.

## Pass Host Header

When you select this option, the host header as requested by the client will be preserved and forwarded along with the web request to the web server. Whether passing the host header is necessary in your environment depends on the configuration of your web server.

**Additional Options**

Disable Compression Support

Rewrite HTML

Pass Host Header

**Figure 268: Advanced**

## 9. Click Save.



**Note:** As soon as a new HTTP based rule configuration has been created and saved or an existing HTTP based rule configuration has been altered and saved, all HTTP based business rules will be restarted. Any underlying client connection using a HTTP based business rule will get lost and has to be re-established.

The Exchange Outlook Anywhere rule has been created and appears on the **Firewall** page when the **IPv4** filter is set.

## Add Rule for Exchange General

(only available for IPv4 policy) This page describes how to configure a rule for Exchange General.

1. Go to **Protect > Firewall** and select **IPv4**. using the filter switch.
2. Click **+Add Firewall Rule** and **Business Application Rule**.
3. Specify the general policy details.

### Application Template

Select **Exchange General** to configure a rule for Exchange General.

### Description

Enter a description for the rule.

### Rule Position

Specify the position of the rule.

**Available Options:** TopBottom

### Rule Name

Specify a name for the rule.

The screenshot shows a configuration interface for a rule. On the left, there's a dropdown for 'Application Template' set to 'Exchange General'. To its right is a 'Description' field containing the placeholder 'Description'. Further right is a 'Rule Position' dropdown set to 'Top'. Below these are two input fields: 'Rule Name \*' with the placeholder 'Rule name' and a larger 'Description' field which is currently empty.

**Figure 269: About This Rule**

- Specify Hosted Server details.

#### Hosted Address

Specify the address of the hosted server to which the rule applies. It is the public IP address through which Internet users access an internal server/host.



**Note:** When a client establishes a connection and accesses the web server, the web server does not obtain the client's real IP address. The server obtains the address of the interface used by the Web Application Firewall (WAF) since the connection is made through the WAF. The client's real IP address is available in the HTTP header

#### Listening Port

Enter a port number on which the hosted web server can be reached externally over the Internet. Default is port 80 for plaintext communication (HTTP) and port 443 for encrypted communication (HTTPS).

#### HTTPS

Select to enable or disable of HTTPS traffic.

#### HTTPS Certificate (*available only if HTTPS is selected*)

Select the HTTPS certificate to be used.

#### Redirect HTTP (*available only if HTTPS is selected*)

Select to redirect HTTP requests.

#### Domains

Use FQDN when you enter the domains the web server is responsible for, for example, shop.example.com.

The screenshot shows a configuration interface for a hosted server. On the left, there's a 'Hosted Address \*' section with a dropdown menu showing 'Address'. Next to it is a 'Listening Port \*' field containing '80'. Below these are two checkboxes: 'HTTPS' (unchecked) and 'Redirect HTTP' (unchecked). On the right, there's a 'Domains \*' section with a 'Search / Add' input field and a '+' button.

**Figure 270: Hosted Server**

- Specify Protected Server(s) details.

#### Path-specific routing

You can enable path-specific routing to define (path) to which web servers incoming requests are forwarded.

You can define that all URLs with a specific path, for example, /products/, are sent to a specific web server. On the other hand you can allow more than one web server for a specific request but add rules how to distribute the requests among the servers. Additionally, you can define that each session is bound to one web server throughout its lifetime (sticky session). This may be necessary if you host an online shop and want to make sure that a user sticks to one server during the shopping

session. You can also configure to send all requests to one web server and use the others only as a backup.

For each hosted web server, one default site path route (with path '/') is created automatically. The device automatically applies the site path routes in the most reasonable way: starting with the strictest, i.e., longest paths and ending with the default path route which is only used if no other more specific site path route matches the incoming request. The order of the site path route list is not relevant. If no route matches an incoming request, (in case the default route was deleted), the request will be denied.

#### Add New Path (*available only if Path-specific routing is selected*)

Click **Add New Path** to define a new path.

##### [Add Path](#)

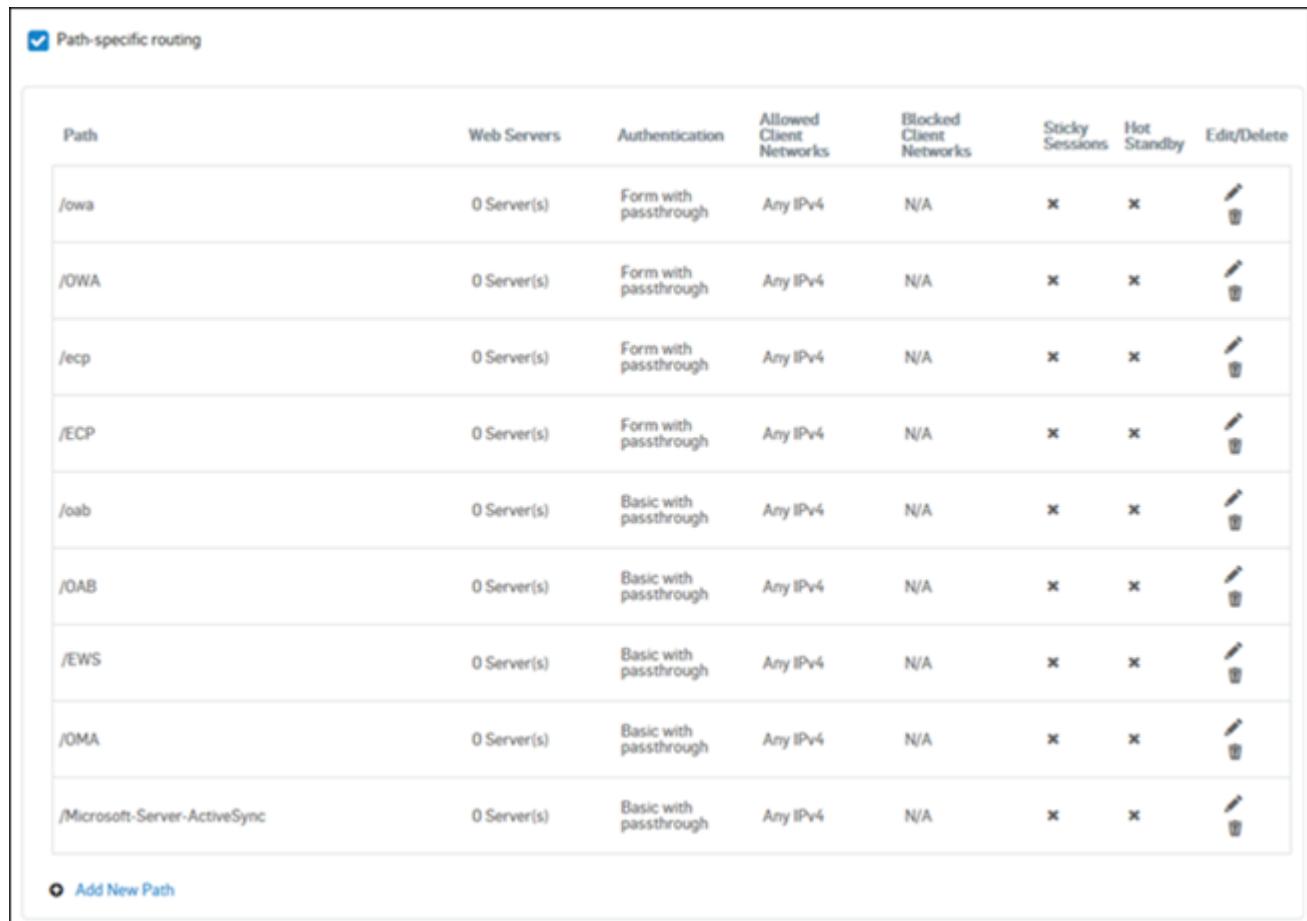
 **Note:** **Add New Path** will only be active after at least one web server and one hosted web server have been created.

Default: /owa, /OWA, /ecp, /ECP, /oab, /OAB, /ews, /EWS, /oma, /OMA, /Microsoft-Server-ActiveSync

#### Web Servers (*not available if Path-specific routing is selected*)

Web servers are the application servers that are to be protected. Select a web server from the list of web servers or click **Add New Item** to add a web server.

A new web server can be created directly from this page or from the **Protect > Web Server > Web Servers** page.



The screenshot shows a configuration interface for 'Protected Server(s)'. At the top left is a checked checkbox labeled 'Path-specific routing'. Below this is a table with the following columns: Path, Web Servers, Authentication, Allowed Client Networks, Blocked Client Networks, Sticky Sessions, Hot Standby, and Edit/Delete. The table lists eight entries corresponding to standard Microsoft Exchange paths: /owa, /OWA, /ecp, /ECP, /oab, /OAB, /ews, and /EWS. Each row shows 0 Server(s) assigned, 'Form with passthrough' authentication, and 'Any IPv4' allowed client networks. The 'Blocked Client Networks' column is 'N/A'. The 'Sticky Sessions' and 'Hot Standby' columns both contain an 'x'. Each row has an edit icon (pencil) and a delete icon (trash bin) in the 'Edit/Delete' column. At the bottom of the table is a blue link labeled 'Add New Path'.

Path	Web Servers	Authentication	Allowed Client Networks	Blocked Client Networks	Sticky Sessions	Hot Standby	Edit/Delete
/owa	0 Server(s)	Form with passthrough	Any IPv4	N/A	x	x	 
/OWA	0 Server(s)	Form with passthrough	Any IPv4	N/A	x	x	 
/ecp	0 Server(s)	Form with passthrough	Any IPv4	N/A	x	x	 
/ECP	0 Server(s)	Form with passthrough	Any IPv4	N/A	x	x	 
/oab	0 Server(s)	Basic with passthrough	Any IPv4	N/A	x	x	 
/OAB	0 Server(s)	Basic with passthrough	Any IPv4	N/A	x	x	 
/ews	0 Server(s)	Basic with passthrough	Any IPv4	N/A	x	x	 
/EWS	0 Server(s)	Basic with passthrough	Any IPv4	N/A	x	x	 
/oma	0 Server(s)	Basic with passthrough	Any IPv4	N/A	x	x	 
/Microsoft-Server-ActiveSync	0 Server(s)	Basic with passthrough	Any IPv4	N/A	x	x	 

**Figure 271: Protected Server(s)**

- Specify Access Permission details. (*not available if Path-specific routing is selected*)

### Allowed Client Networks

Select the allowed host(s)/network(s).

### Blocked Client Networks

Select the blocked host(s)/network(s).

### Authentication

Select the web application authentication profile from the list of available profiles. You can also create new authentication profile on this page or on the **Protect > Web Server > Authentication Policies** page.

The screenshot shows a configuration interface for access permissions. It has three main sections: 'Allowed Client Networks' containing a dropdown menu 'Any IPv4' and a 'Add New Item' button; 'Blocked Client Networks' containing a 'Add New Item' button; and 'Authentication' with a dropdown menu set to 'None'.

**Figure 272: Access Permission**

- Add path Exceptions for the web servers.

Click **Add New Exception** to specify a new exception.

*Add Exception*

Default: /owa/\*,/OWA/\*,/ews/\*,/EWS/\*,/ecp/\*,/ECP/\*,/oab/\*,/OAB/\*,/oma/\*,/OMA/\*,/Microsoft-Server-ActiveSync?\*,/owa/ev.owa\*

The screenshot shows a table of exceptions. The columns are Path, Client Resource, Checks, Categories, Status, and Edit/Delete. There are two entries: one for '/owa/\*,/OWA/\*,/ews/\*,/EWS/\*,/ecp/\*,/ECP/\*,/oab/\*,/OAB/\*,/oma/\*,/OMA/\*,/Microsoft-Server-ActiveSync?\*' with status ON, and another for '/owa/ev.owa\*' with status ON. At the bottom left is a blue button labeled '+ ADD NEW EXCEPTION'.

Path	Client Resource	Checks	Categories	Status	Edit/Delete
/owa/*,/OWA/*,/ews/*,/EWS/*,/ecp/*,/ECP/*,/oab/*,/OAB/*,/oma/*,/OMA/*,/Microsoft-Server-ActiveSync?*	N/A	1	0	ON <input checked="" type="button"/>	
/owa/ev.owa*	N/A	1	11	ON <input checked="" type="button"/>	

**Figure 273: Exceptions**

- Specify Advanced settings.
  - Specify **Policies** for Business Applications.

### Protection

Select an application protection policy for the server or create a new one. A new application protection policy can be created directly from this page or from the **Protect > Web Server > Protection Policies** page. You can also choose to have **None** application protection.

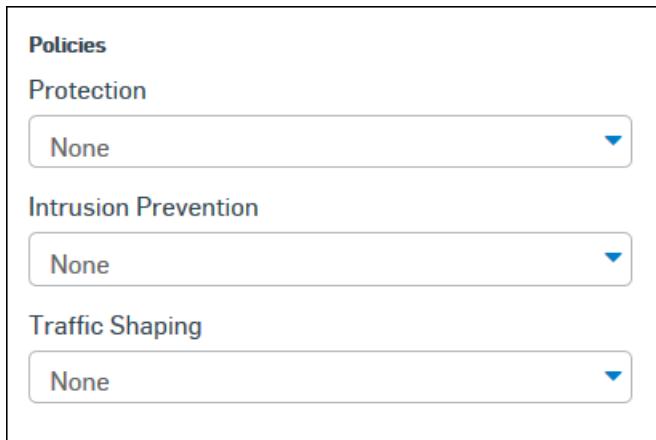
### Intrusion Prevention

Select an Intrusion Prevention policy for the rule or create a new one. A new IPS policy can be created directly from this page or from the **Protect > Intrusion Prevention > IPS Policies** page. You can also choose to have **None** intrusion prevention.

### Traffic Shaping

The traffic shaping policy allocates & limits the maximum bandwidth usage of the user.

Select a traffic shaping policy for the rule or create a new one. A new traffic shaping policy can be created directly from this page or from the **System > System Services > Traffic Shaping** page. You can also choose to have **None** traffic shaping.



**Figure 274: Policies for Business Applications**

- Specify **Additional Options** for the added server.

#### Disable Compression Support

By default, this check box is disabled and the content is sent compressed when the client requests compressed data. Compression increases transmission speed and reduces page load time. However, if websites are displayed incorrectly or users experience content-encoding errors when accessing your web servers, it may be necessary to disable compression. When the check box is enabled, the WAF will request uncompressed data from the web servers of this hosted web server and will send it uncompressed to the client, independent of the HTTP request's encoding parameter.

#### Rewrite HTML

Select this option to have the device rewrite links of the returned webpages in order for the links to stay valid. Example: One of your web server instances has the hostname `yourcompany.local` but the hosted web server's hostname on the device is `yourcompany.com`. Thus, absolute links like `[a href="http://yourcompany.local/"]` will be broken if the link is not rewritten to `[a href="http://yourcompany.com/"]` before delivery to the client. However, you do not need to enable this option if either `yourcompany.com` is configured on your web server or if internal links on your webpages are always realized as relative links. It is recommended to use the option with Microsoft's Outlook web access and/or SharePoint portal server.



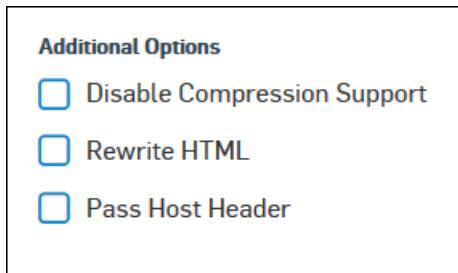
**Note:** HTML rewriting affects all files with a HTTP content type of `text/*` or `*xml*`, where `*` is a wildcard. Make sure that other file types, e.g. binary files, have the correct HTTP content type, otherwise they may get corrupted by the HTML rewriting process.

#### Rewrite cookies (*available only if Rewrite HTML is selected*)

Select this option to have the device rewrite cookies of the returned web pages.

#### Pass Host Header

When you select this option, the host header as requested by the client will be preserved and forwarded along with the web request to the web server. Whether passing the host header is necessary in your environment depends on the configuration of your web server.



**Figure 275: Advanced**

**9. Click Save.**



**Note:** As soon as a new HTTP based rule configuration has been created and saved or an existing HTTP based rule configuration has been altered and saved, all HTTP based business rules will be restarted. Any underlying client connection using a HTTP based business rule will get lost and has to be re-established.

The Exchange General rule has been created and appears on the **Firewall** page when the **IPv4** filter is set.

**Add Rule for Microsoft Lync**

(only available for IPv4 policy) This page describes how to configure a rule for Microsoft Lync.

1. Go to **Protect > Firewall** and select **IPv4**. using the filter switch.
2. Click **+Add Firewall Rule** and **Business Application Rule**.
3. Specify the general rule details.

**Application Template**

Select **Microsoft Lync** to define Application filter policy for HTTP based applications.

**Description**

Enter a description for the rule.

**Rule Position**

Specify the position of the rule.

**Available Options:**

- Top
- Bottom

**Rule Name**

Specify a name to identify the rule.

Application Template	Description	Rule Position
Microsoft Lync	Description	Top
Rule Name *		
Rule name		

**Figure 276: About This Rule**

**4. Specify Hosted Server details.**

**Hosted Address**

Specify the address of the hosted server to which the rule applies. It is the public IP address through which Internet users access internal server/host.



**Note:** When a client establishes a connection and accesses the web server, the web server does not obtain the client's real IP address. The server obtains the address of the interface used by the Web Application Firewall (WAF) since the connection is made through the WAF. The client's real IP address is available in the HTTP header

**Listening Port**

Enter a port number on which the hosted web server can be reached externally over the Internet. Default is port 80 for plaintext communication (HTTP) and port 443 for encrypted communication (HTTPS).

### HTTPS

Click to enable or disable of HTTPS traffic.

#### HTTPS Certificate (*available if HTTPS is enabled*)

Select the HTTPS certificate to be used.

#### Redirect HTTP (*available if HTTPS is enabled*)

Click to redirect HTTP requests.

### Domains

Use FQDN when you enter the domains the web server is responsible for, for example, shop.example.com.

The screenshot shows a configuration form for a hosted server. It includes fields for 'Hosted Address \*' (with a dropdown menu for 'Address'), 'Listening Port \*' (set to 80), and a checkbox for 'HTTPS'. Below these are two additional checkboxes: 'Redirect HTTP' and a plus sign icon for adding more domains. To the right is a section labeled 'Domains \*' with a search bar and a plus sign icon for adding domains.

**Figure 277: Hosted Server**

**5. Specify Protected Server(s) details.**

#### Path-specific routing

You can enable path-specific routing to define (the path) to which web servers incoming requests are forwarded.

You can define that all URLs with a specific path, for example, /products/, are sent to a specific web server. On the other hand you can allow more than one web server for a specific request but add rules how to distribute the requests among the servers. Additionally, you can define that each session is bound to one web server throughout its lifetime (sticky session). This may be necessary if you host an online shop and want to make sure that a user sticks to one server during the shopping session. You can also configure to send all requests to one web server and use the others only as a backup.

For each hosted web server, one default site path route (with path '/') is created automatically. The device automatically applies the site path routes in the most reasonable way: starting with the strictest, i.e., longest paths and ending with the default path route which is only used if no other more specific site path route matches the incoming request. The order of the site path route list is not relevant. If no route matches an incoming request, (in case the default route was deleted), the request will be denied.

#### Add New Path (*available if Path-specific routing is enabled*)

Click **Add Path** to define a new path.

##### [Add Path](#)

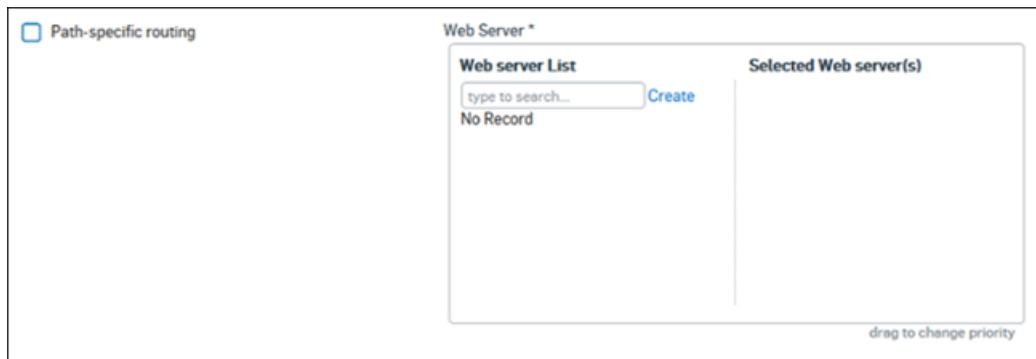


**Note:** **Add New Path** will only be active after at least one web server and one hosted web server have been created.

#### Web Server (*available if Path-specific routing is disabled*)

Hosts are the web servers that are to be protected. Select a web server from the list of web servers or click **Add New Item** to add a web server.

A new web server can be created directly from this page or from the **Protect > Web Server > Web Servers** page.



**Figure 278: Protected Application Server(s)**

- Specify Access Permission details (*not available if Path-specific routing is selected*).

#### Allowed Client Networks

Select the allowed host(s)/network(s).

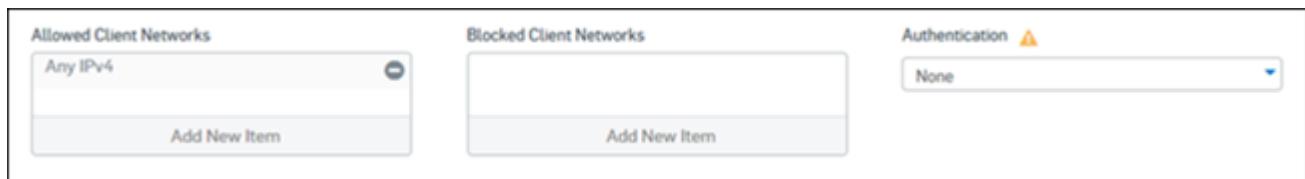
#### Blocked Client Networks

Select the blocked host(s)/network(s).

#### Authentication

Select the web application authentication profile from the list of available profiles.

You can also create a new authentication profile on this page or on the **Protect > Web Server > Authentication Policies** page.



**Figure 279: Access Permission**

- Specify path Exceptions for the web servers.

Click **Add New Exception** to specify a new exception.

[Add Exception](#)



**Figure 280: Exceptions**

- Specify Advanced settings.
  - Specify Policies for Business Applications.

#### Protection

Select an application protection policy for the server or create a new one. A new application protection policy can be created directly from this page or from the **Protect > Web Server > Protection Policies** page. You can also choose to have **None** application protection.

#### Intrusion Prevention

Select an Intrusion Prevention policy for the rule or create a new one. A new IPS policy can be created directly from this page or from the **Protect > Intrusion Prevention > IPS Policies** page. You can also choose to have **None** intrusion prevention.

## Traffic Shaping

The traffic shaping policy allocates & limits the maximum bandwidth usage of the user.

Select a traffic shaping policy for the rule or create a new one. A new traffic shaping policy can be created directly from this page or from the **System > System Services > Traffic Shaping** page. You can also choose to have **None** traffic shaping.

The screenshot shows a configuration interface for policies. It has three main sections with dropdown menus:

- Policies**: Protection dropdown set to **None**.
- Intrusion Prevention**: dropdown set to **None**.
- Traffic Shaping**: dropdown set to **None**.

**Figure 281: Policies for Business Applications**

- Specify **Additional Options** for the added server.

### Disable Compression Support

By default, this check box is disabled and the content is sent compressed when the client requests compressed data. Compression increases transmission speed and reduces page load time. However, if websites are displayed incorrectly or users experience content-encoding errors when accessing your web servers, it may be necessary to disable compression. When the check box is enabled, the WAF will request uncompressed data from the web servers of this hosted web server and will send it uncompressed to the client, independent of the HTTP request's encoding parameter.

### Rewrite HTML

Select this option to have the device rewrite links of the returned webpages in order for the links to stay valid. Example: One of your web server instances has the hostname `yourcompany.local` but the hosted web server's hostname on the device is `yourcompany.com`. Thus, absolute links like `[a href="http://yourcompany.local/"]` will be broken if the link is not rewritten to `[a href="http://yourcompany.com/"]` before delivery to the client. However, you do not need to enable this option if either `yourcompany.com` is configured on your web server or if internal links on your webpages are always realized as relative links. It is recommended to use the option with Microsoft's Outlook web access and/or SharePoint portal server.



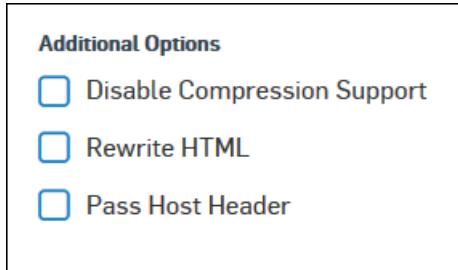
**Note:** HTML rewriting affects all files with a HTTP content type of `text/*` or `*xml*`, where `*` is a wildcard. Make sure that other file types, e.g. binary files, have the correct HTTP content type, otherwise they may get corrupted by the HTML rewriting process.

### Rewrite cookies (*available only if Rewrite HTML is selected*)

Select this option to have the device rewrite cookies of the returned web pages.

### Pass Host Header

When you select this option, the host header as requested by the client will be preserved and forwarded along with the web request to the web server. Whether passing the host header is necessary in your environment depends on the configuration of your web server.



**Figure 282: Advanced**

9. Click **Save**.



**Note:** As soon as a new HTTP based rule configuration has been created and saved or an existing HTTP based rule configuration has been altered and saved, all HTTP based business rules will be restarted. Any underlying client connection using a HTTP based business rule will get lost and has to be re-established.

The Microsoft Lync rule has been created and appears on the **Firewall** page when the **IPv4** filter is set.

#### Add Rule for Microsoft Remote Desktop Gateway 2008 and R2

(only available for IPv4 policy) This page describes how to configure a rule for Microsoft Remote Desktop Gateway 2008 and R2.

1. Go to **Protect > Firewall** and select **IPv4**. using the filter switch.
2. Click **+Add Firewall Rule** and **Business Application Rule**.
3. Specify the general rule details.

#### Application Template

Select **Microsoft Remote Desktop Gateway 2008 and R2** to configure a rule for Microsoft Remote Desktop Gateway 2008 and R2.

#### Description

Enter a description for the rule.

#### Rule Position

Specify the position of the rule.

#### Available Options:

- Top
- Bottom

#### Rule Name

Specify a name to identify the rule.

Application Template	Description	Rule Position
Microsoft Remote Desktop Gateway 2008 and R2	Description	Top
Rule Name *	Rule name	

**Figure 283: About This Rule**

4. Specify **Hosted Server** details.

#### Hosted Address

Specify the address of the hosted server to which the rule applies. It is the public IP address through which Internet users access an internal server/host.



**Note:** When a client establishes a connection and accesses the web server, the web server does not obtain the client's real IP address. The server obtains the address of the interface used by the Web Application Firewall (WAF) since the connection is made through the WAF. The client's real IP address is available in the HTTP header

## Listening Port

Enter a port number on which the hosted web server can be reached externally, over the Internet. Default is port 80 for plaintext communication (HTTP) and port 443 for encrypted communication (HTTPS).

## HTTPS

Click to enable or disable of HTTPS traffic.

### HTTPS Certificate (*available if HTTPS is enabled*)

Select the HTTPS certificate to be used.

### Redirect HTTP (*available if HTTPS is enabled*)

Click to redirect HTTP requests.

## Domains

Use FQDN when you enter the domains the web server is responsible for, for example, shop.example.com.

The screenshot shows a configuration form for a hosted server. It includes fields for 'Hosted Address \*' (with a dropdown menu), 'Listening Port \*' (set to 80), and a checkbox for 'HTTPS'. Below these are checkboxes for 'HTTPS' (which is checked) and 'Redirect HTTP' (which is unchecked). On the right side, there is a 'Domains \*' section with a 'Search / Add' input field and a '+' button. The entire form is enclosed in a light gray border.

**Figure 284: Hosted Server**

## 5. Specify Protected Server(s) details.

### Path-specific routing

You can enable path-specific routing to define (a path) to which web servers incoming requests are forwarded.

You can define that all URLs with a specific path, for example, /products/, are sent to a specific web server. On the other hand you can allow more than one web server for a specific request but add rules how to distribute the requests among the servers. Additionally, you can define that each session is bound to one web server throughout its lifetime (sticky session). This may be necessary if you host an online shop and want to make sure that a user sticks to one server during the shopping session. You can also configure to send all requests to one web server and use the others only as a backup.

For each hosted web server, one default site path route (with path '/') is created automatically. The device automatically applies the site path routes in the most reasonable way: starting with the strictest, i.e., longest paths and ending with the default path route which is only used if no other more specific site path route matches the incoming request. The order of the site path route list is not relevant. If no route matches an incoming request, (in case the default route was deleted), the request will be denied.

### Add New Path (*available if Path-specific routing is enabled*)

Click **Add New Path** to define a new path.

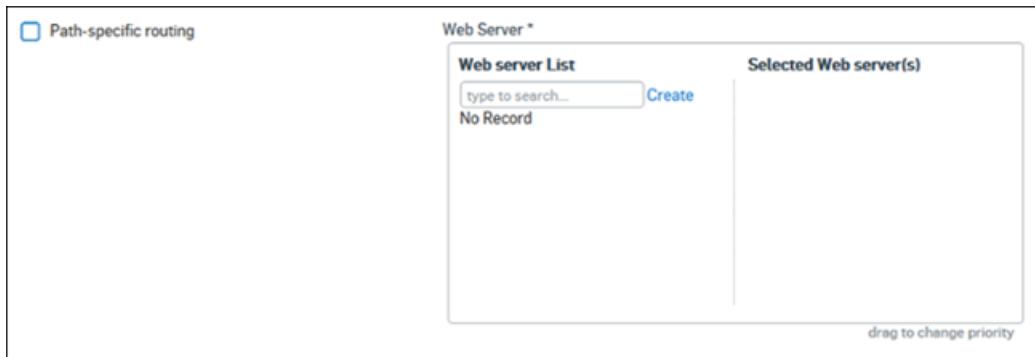
[Add Path](#)

**Note:** **Add New Path** will only be active after at least one web server and one hosted web server have been created.

### Web Server (*available if Path-specific routing is disabled*)

Web servers are the application servers that are to be protected. Select from the list of web servers or click **Add New Item** to add a web server.

A new web server can be created directly from this page or from the **Protect > Web Server > Web Servers** page.



**Figure 285: Protected Server(s)**

- Specify access permission details. (*Available if Path-specific routing is disabled*)

#### Allowed Client Networks

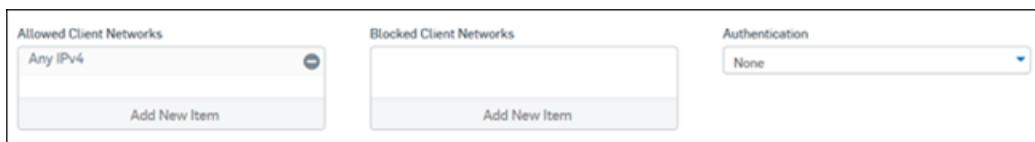
Select the allowed host(s)/network(s).

#### Blocked Client Networks

Select the blocked host(s)/network(s).

#### Authentication

Select the web application authentication profile from the list of available profiles. You can also create a new authentication profile from this page or from the **Protect > Web Server > Authentication Policies** page.



**Figure 286: Access Permission**

- Specify path **Exceptions** for the web servers.

Click **Add New Exception** to specify new exception.

*Add Exception*



**Figure 287: Exceptions**

- Specify Advanced settings.

- Specify **Policies** for Business Applications.

#### Protection

Select an application protection policy for the server or create a new one. A new application protection policy can be created directly from this page or from the **Protect > Web Server > Protection Policies** page. You can also choose to have **None** application protection.

#### Intrusion Prevention

Select an Intrusion Prevention policy for the rule or create a new one. A new IPS policy can be created directly from this page or from the **Protect > Intrusion Prevention > IPS Policies** page. You can also choose to have **None** intrusion prevention.

## Traffic Shaping

The traffic shaping policy allocates & limits the maximum bandwidth usage of the user.

Select a traffic shaping policy for the rule or create a new one. A new traffic shaping policy can be created directly from this page or from the **System > System Services > Traffic Shaping** page. You can also choose to have **None** traffic shaping.

The screenshot shows a configuration interface for policies. It has three main sections with dropdown menus:

- Policies**: Protection dropdown set to **None**.
- Intrusion Prevention**: dropdown set to **None**.
- Traffic Shaping**: dropdown set to **None**.

**Figure 288: Policies for Business Applications**

- Specify **Additional Options** for the added server.

### Disable Compression Support

By default, this check box is disabled and the content is sent compressed when the client requests compressed data. Compression increases transmission speed and reduces page load time. However, if websites are displayed incorrectly or users experience content-encoding errors when accessing your web servers, it may be necessary to disable compression. When the check box is enabled, the WAF will request uncompressed data from the web servers of this hosted web server and will send it uncompressed to the client, independent of the HTTP request's encoding parameter.

### Rewrite HTML

Select this option to have the device rewrite links of the returned webpages in order for the links to stay valid. Example: One of your web server instances has the hostname `yourcompany.local` but the hosted web server's hostname on the device is `yourcompany.com`. Thus, absolute links like `[a href="http://yourcompany.local/"]` will be broken if the link is not rewritten to `[a href="http://yourcompany.com/"]` before delivery to the client. However, you do not need to enable this option if either `yourcompany.com` is configured on your web server or if internal links on your webpages are always realized as relative links. It is recommended to use the option with Microsoft's Outlook web access and/or SharePoint portal server.



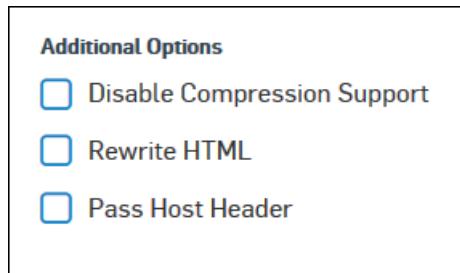
**Note:** HTML rewriting affects all files with a HTTP content type of `text/*` or `*xml*`, where `*` is a wildcard. Make sure that other file types, e.g. binary files, have the correct HTTP content type, otherwise they may get corrupted by the HTML rewriting process.

### Rewrite cookies (*available only if Rewrite HTML is selected*)

Select this option to have the device rewrite cookies of the returned web pages.

### Pass Host Header

When you select this option, the host header as requested by the client will be preserved and forwarded along with the web request to the web server. Whether passing the host header is necessary in your environment depends on the configuration of your web server.



**Figure 289: Advanced**

9. Click **Save**.



**Note:** As soon as a new HTTP based rule configuration has been created and saved or an existing HTTP based rule configuration has been altered and saved, all HTTP based business rules will be restarted. Any underlying client connection using a HTTP based business rule will get lost and has to be re-established.

The rule for Microsoft Remote Desktop Gateway 2008 and R2 has been created and appears on the **Firewall** page when the **IPv4** filter is set.

### Add Rule for Microsoft Remote Desktop Web 2008 and R2

(only available for IPv4 policy) This page describes how to configure a rule for Microsoft Remote Desktop Web 2008 and R2.

1. Go to **Protect > Firewall** and select **IPv4**. using the filter switch.
2. Click **+Add Firewall Rule** and **Business Application Rule**.
3. Specify the general rule details.

#### Application Template

Select **Microsoft Remote Desktop Web 2008 and R2** to configure a rule for Microsoft Remote Desktop Web 2008 and R2.

#### Description

Enter a description for the rule.

#### Rule Position

Specify the position of the rule.

**Available Options:** TopBottom

#### Rule Name

Specify a name to identify the rule.

Application Template	Description	Rule Position
Microsoft Remote Desktop Web 2008 and R2	Description	Top
Rule Name *		
Rule name		

**Figure 290: About This Rule**

4. Specify **Hosted Server** details.

#### Hosted Address

Specify the address of the hosted server to which the rule applies. It is the public IP address through which Internet users access an internal server/host.



**Note:** When a client establishes a connection and accesses the web server, the web server does not obtain the client's real IP address. The server obtains the address of the interface used by the Web Application Firewall (WAF) since the connection is made through the WAF. The client's real IP address is available in the HTTP header

#### Listening Port

Enter a port number on which the hosted web server can be reached externally over the Internet. Default is port 80 for plaintext communication (HTTP) and port 443 for encrypted communication (HTTPS).

### HTTPS

Click to enable or disable of HTTPS traffic.

#### HTTPS Certificate (*available if HTTPS is enabled*)

Select the HTTPS certificate to be used.

#### Redirect HTTP (*available if HTTPS is enabled*)

Click to redirect HTTP requests.

### Domains

Use FQDN when you enter the domains the web server is responsible for, for example, shop.example.com.

The screenshot shows a configuration form for a hosted server. On the left, there's a dropdown menu for 'Hosted Address \*' with 'Address' selected. Next to it is a 'Listening Port \*' field containing '80'. Below these are two checkboxes: 'HTTPS' (unchecked) and 'Redirect HTTP' (unchecked). On the right, there's a 'Domains \*' section with a list box containing no entries. At the bottom of this section is a 'Search / Add' input field and a blue '+' button.

**Figure 291: Hosted Server**

**5. Specify Protected Server(s) details.**

#### Path-specific routing

You can enable path-specific routing to define (the path) to which web servers incoming requests are forwarded.

You can define that all URLs with a specific path, for example, /products/, are sent to a specific web server. On the other hand you can allow more than one web server for a specific request but add rules how to distribute the requests among the servers. Additionally, you can define that each session is bound to one web server throughout its lifetime (sticky session). This may be necessary if you host an online shop and want to make sure that a user sticks to one server during the shopping session. You can also configure to send all requests to one web server and use the others only as a backup.

For each hosted web server, one default site path route (with path '/') is created automatically. The device automatically applies the site path routes in the most reasonable way: starting with the strictest, i.e., longest paths and ending with the default path route which is only used if no other more specific site path route matches the incoming request. The order of the site path route list is not relevant. If no route matches an incoming request, (in case the default route was deleted), the request will be denied.

#### Add New Path (*available if Path-specific routing is enabled*)

Click **Add New Path** to define a new path.

##### [Add Path](#)

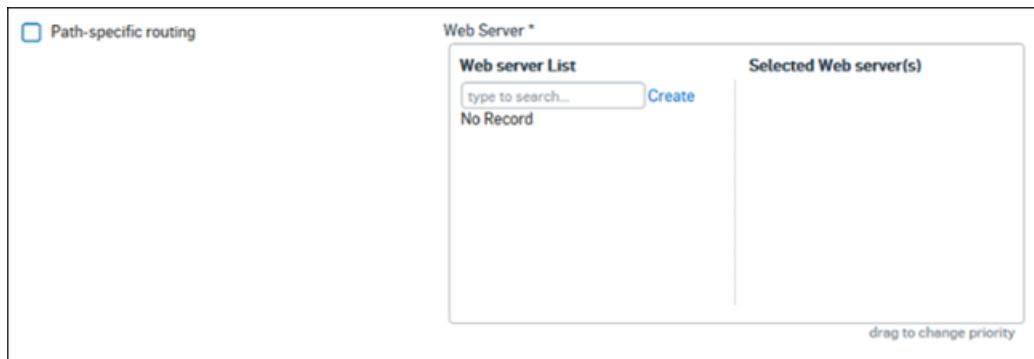


**Note:** **Add New Path** will only be active after at least one web server and one hosted web server have been created.

#### Web Server (*available if Path-specific routing is disabled*)

Web servers are the application servers that are to be protected. Select a web server from the list of web servers or click **Add New Item** to add a web server.

A new web server can be created directly on this page or on the **Protect > Web Server > Web Servers** page.



**Figure 292: Protected Server(s)**

- Specify **Access Permission** details (*available if Path-specific routing is disabled*).

#### Allowed Client Networks

Select the allowed host(s)/network(s).

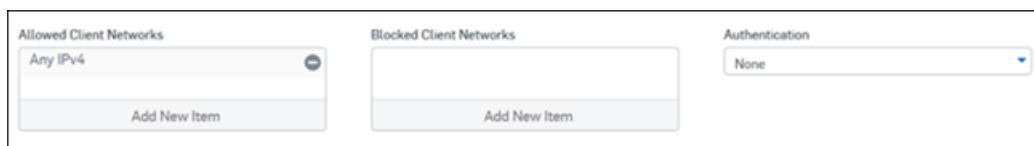
#### Blocked Client Networks

Select the blocked host(s)/network(s).

#### Authentication

Select the web application authentication profile from the list of available profiles.

You can also create new authentication profile on this page or on the **Protect > Web Server > Authentication Policies** page.



**Figure 293: Access Permission**

- Add path **Exceptions** for the web servers.

Click **Add New Exception** to specify new exception.

[Add Exception](#)



**Figure 294: Exceptions**

- Specify Advanced settings.

- Specify **Policies** for Business Applications.

#### Protection

Select an application protection policy for the server or create a new one. A new application protection policy can be created directly from this page or from the **Protect > Web Server > Protection Policies** page. You can also choose to have **None** application protection.

#### Intrusion Prevention

Select an Intrusion Prevention policy for the rule or create a new one. A new IPS policy can be created directly from this page or from the **Protect > Intrusion Prevention > IPS Policies** page. You can also choose to have **None** intrusion prevention.

#### Traffic Shaping

The traffic shaping policy allocates & limits the maximum bandwidth usage of the user.

Select a traffic shaping policy for the rule or create a new one. A new traffic shaping policy can be created directly from this page or from the **System > System Services > Traffic Shaping** page. You can also choose to have **None** traffic shaping.



**Figure 295: Policies for Business Applications**

- Specify **Additional Options** for the added server.

#### Disable Compression Support

By default, this check box is disabled and the content is sent compressed when the client requests compressed data. Compression increases transmission speed and reduces page load time. However, if websites are displayed incorrectly or users experience content-encoding errors when accessing your web servers, it may be necessary to disable compression. When the check box is enabled, the WAF will request uncompressed data from the web servers of this hosted web server and will send it uncompressed to the client, independent of the HTTP request's encoding parameter.

#### Rewrite HTML

Select this option to have the device rewrite links of the returned webpages in order for the links to stay valid. Example: One of your web server instances has the hostname `yourcompany.local` but the hosted web server's hostname on the device is `yourcompany.com`. Thus, absolute links like `[a href="http://yourcompany.local/"]` will be broken if the link is not rewritten to `[a href="http://yourcompany.com/"]` before delivery to the client. However, you do not need to enable this option if either `yourcompany.com` is configured on your web server or if internal links on your webpages are always realized as relative links. It is recommended to use the option with Microsoft's Outlook web access and/or SharePoint portal server.



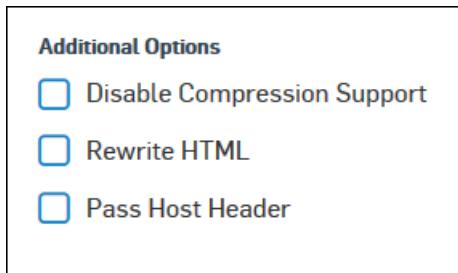
**Note:** HTML rewriting affects all files with a HTTP content type of `text/*` or `*xml*`, where `*` is a wildcard. Make sure that other file types, e.g. binary files, have the correct HTTP content type, otherwise they may get corrupted by the HTML rewriting process.

#### Rewrite cookies (*available only if Rewrite HTML is selected*)

Select this option to have the device rewrite cookies of the returned web pages.

#### Pass Host Header

When you select this option, the host header as requested by the client will be preserved and forwarded along with the web request to the web server. Whether passing the host header is necessary in your environment depends on the configuration of your web server.



**Figure 296: Advanced**

9. Click **Save**.



**Note:** As soon as a new HTTP based rule configuration has been created and saved or an existing HTTP based rule configuration has been altered and saved, all HTTP based business rules will be restarted. Any underlying client connection using a HTTP based business rule will get lost and has to be re-established.

The rule for Microsoft Remote Desktop Web 2008 and R2 has been created and appears on the **Firewall** page when the **IPv4** filter is set.

### Add Rule for Microsoft Sharepoint 2010 and 2013

(only available for IPv4 policy) This page describes how to configure a rule for Microsoft SharePoint 2010 and 2013.

1. Go to **Protect > Firewall** and select **IPv4**. using the filter switch.
2. Click **+Add Firewall Rule** and **Business Application Rule**.
3. Specify the general rule details.

#### Application Template

Select **Microsoft Sharepoint 2010 and 2013** to configure a rule for Microsoft Sharepoint 2010 and 2013.

#### Description

Enter a description for the rule.

#### Rule Position

Specify the position of the rule.

#### Available Options:

- Top
- Bottom

#### Rule Name

Specify a name to identify the rule.

Application Template	Description	Rule Position
Microsoft Sharepoint 2010 and 2013	Description	Top
Rule Name *		
Rule name		

**Figure 297: About This Rule**

4. Specify **Hosted Server** details.

#### Hosted Address

Specify the address of the hosted server to which the rule applies. It is the public IP address through which Internet users access an internal server/host.



**Note:** When a client establishes a connection and accesses the web server, the web server does not obtain the client's real IP address. The server obtains the address of the interface used by the Web Application Firewall (WAF) since the connection is made through the WAF. The client's real IP address is available in the HTTP header

## Listening Port

Enter a port number on which the hosted web server can be reached externally over the Internet. Default is port 80 for plaintext communication (HTTP) and port 443 for encrypted communication (HTTPS).

## HTTPS

Click to enable or disable of HTTPS traffic.

### HTTPS Certificate (*available if HTTPS is enabled*)

Select the HTTPS certificate to be used.

### Redirect HTTP (*available if HTTPS is enabled*)

Click to redirect HTTP requests.

## Domains

Use FQDN when you enter the domains the web server is responsible for, for example, shop.example.com.

The screenshot shows a configuration form for a hosted server. It includes fields for 'Hosted Address \*' (with a dropdown menu), 'Listening Port \*' (set to 80), and a checkbox for 'HTTPS'. Below these are checkboxes for 'Redirect HTTP' and 'Domains \*' (with a search bar and a '+' button). The entire form is enclosed in a light gray border.

**Figure 298: Hosted Server**

## 5. Specify Protected Server(s) details.

### Path-specific routing

You can enable path-specific routing to define (a path) to which web servers incoming requests are forwarded.

You can define that all URLs with a specific path, for example, /products/, are sent to a specific web server. On the other hand you can allow more than one web server for a specific request but add rules how to distribute the requests among the servers. Additionally, you can define that each session is bound to one web server throughout its lifetime (sticky session). This may be necessary if you host an online shop and want to make sure that a user sticks to one server during the shopping session. You can also configure to send all requests to one web server and use the others only as a backup.

For each hosted web server, one default site path route (with path '/') is created automatically. The device automatically applies the site path routes in the most reasonable way: starting with the strictest, i.e., longest paths and ending with the default path route which is only used if no other more specific site path route matches the incoming request. The order of the site path route list is not relevant. If no route matches an incoming request, (in case the default route was deleted), the request will be denied.

### Add New Path (*available if Path-specific routing is enabled*)

Click **Add New Path** to define a new path.

[Add Path](#)

**Note:** **Add New Path** will only be active after at least one web server and one hosted web server have been created.

### Web Server (*available if Path-specific routing is disabled*)

Web servers are the application servers that are to be protected. Select a web server from the list of web servers or click **Add New Item** to add a web server.

A new web server can be created directly from this page or from the **Protect > Web Server > Web Servers** page.

**Figure 299: Protected Application Server(s)**

- Specify Access Permission details (*available if Path-specific routing is disabled*).

#### Allowed Client Networks

Select the allowed host(s)/network(s).

#### Blocked Client Networks

Select the blocked host(s)/network(s).

#### Authentication

Select the web application authentication profile from the list of available profiles.

You can also create new authentication profile from this page or from the **Protect > Web Server > Authentication Policies** page.

**Figure 300: Access Permission**

- Add path **Exceptions** for the web servers.

Click **Add New Exception** to specify new exception.

*Add Exception*

**Figure 301: Exceptions**

- Specify Advanced settings.

- Specify **Policies** for Business Applications.

#### Protection

Select an application protection policy for the server or create a new one. A new application protection policy can be created directly from this page or from the **Protect > Web Server > Protection Policies** page. You can also choose to have **None** application protection.

#### Intrusion Prevention

Select an Intrusion Prevention policy for the rule or create a new one. A new IPS policy can be created directly from this page or from the **Protect > Intrusion Prevention > IPS Policies** page. You can also choose to have **None** intrusion prevention.

### Traffic Shaping

The traffic shaping policy allocates & limits the maximum bandwidth usage of the user.

Select a traffic shaping policy for the rule or create a new one. A new traffic shaping policy can be created directly from this page or from the **System > System Services > Traffic Shaping** page. You can also choose to have **None** traffic shaping.

The screenshot shows a configuration window titled 'Policies'. It contains three sections with dropdown menus: 'Protection' set to 'None', 'Intrusion Prevention' set to 'None', and 'Traffic Shaping' set to 'None'. Each section has a small downward arrow icon to its right.

**Figure 302: Policies for Business Applications**

- Specify **Additional Options** for the added server.

### Disable Compression Support

By default, this check box is disabled and the content is sent compressed when the client requests compressed data. Compression increases transmission speed and reduces page load time. However, if websites are displayed incorrectly or users experience content-encoding errors when accessing your web servers, it may be necessary to disable compression. When the check box is enabled, the WAF will request uncompressed data from the web servers of this hosted web server and will send it uncompressed to the client, independent of the HTTP request's encoding parameter.

### Rewrite HTML

Select this option to have the device rewrite links of the returned webpages in order for the links to stay valid. Example: One of your web server instances has the hostname `yourcompany.local` but the hosted web server's hostname on the device is `yourcompany.com`. Thus, absolute links like `[a href="http://yourcompany.local/"]` will be broken if the link is not rewritten to `[a href="http://yourcompany.com/"]` before delivery to the client. However, you do not need to enable this option if either `yourcompany.com` is configured on your web server or if internal links on your webpages are always realized as relative links. It is recommended to use the option with Microsoft's Outlook web access and/or SharePoint portal server.



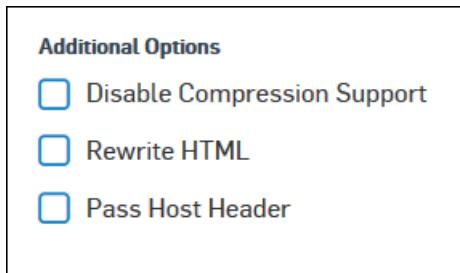
**Note:** HTML rewriting affects all files with a HTTP content type of `text/*` or `*xml*`, where `*` is a wildcard. Make sure that other file types, e.g. binary files, have the correct HTTP content type, otherwise they may get corrupted by the HTML rewriting process.

### Rewrite cookies (*available only if Rewrite HTML is selected*)

Select this option to have the device rewrite cookies of the returned web pages.

### Pass Host Header

When you select this option, the host header as requested by the client will be preserved and forwarded along with the web request to the web server. Whether passing the host header is necessary in your environment depends on the configuration of your web server.



**Figure 303: Advanced**

**9. Click Save.**



**Note:** As soon as a new HTTP based rule configuration has been created and saved or an existing HTTP based rule configuration has been altered and saved, all HTTP based business rules will be restarted. Any underlying client connection using a HTTP based business rule will get lost and has to be re-established.

The rule for Microsoft Sharepoint 2010 and 2013 has been created and appears on the **Firewall** page when the **IPv4** filter is set.

**Add Path**

(only available for the HTTP based business application rules) This page describes how to define a path to which real web servers incoming requests are forwarded.

1. Enable path-specific routing and click **Add New Path**.
2. Specify the path details.

**Path**

Enter the path for which you want to create the site path route.

Example: /products/.

**Web Server**

Select the web servers which are to be used for the specified path.

**Authentication**

Select the web app authentication profile. Select **Create new** to create a new authentication profile.

You can also create an authentication profile from the **Protect > Web Server > Authentication Policies** page.

[Add Authentication Policy](#) on page 494

**Allowed Client Networks**

Select or add the allowed networks that should be able to connect to the hosted web server.

**Blocked Client Networks**

Select or add the denied networks that should be blocked to your hosted web server.

**Sticky session cookie**

Ensures that each session is bound to one web server. If enabled, a cookie is passed to the user's browser, which causes Sophos XG Firewall to route all requests from this browser to the same real web server. If the server is not available, the cookie will be updated, and the session will switch to another web server.

**Hot-standby mode**

Enable if you want to send all requests to the first selected web server, and use the other web servers only as a backup. The backup servers are only used in case the main server fails.

As soon as the main server starts functioning, the sessions will switch back - unless you have selected the **Sticky session cookie** option.

**WebSocket passthrough**

If enabled, applications hosted on the defined site path are allowed to use the WebSocket protocol. WebSocket traffic will be just passed through, it will not be protected in any way.

The screenshot shows the 'Add New Path' configuration page. It includes the following fields:

- Path \***: An input field containing a placeholder 'Path'.
- Web Server \***: A dropdown menu showing 'Selected Web server(s)' and a 'drag to change priority' instruction. Below it is a 'Web server List' panel with a search bar and a message 'No Record'.
- Authentication**: A dropdown menu set to 'None'.
- Allowed Client Networks**: A dropdown menu set to 'Any IPv4' with an 'Add New Item' button below it.
- Blocked Client Networks**: A dropdown menu with an 'Add New Item' button below it.
- Sticky session cookie**: A toggle switch labeled 'OFF' with an information icon.
- Hot standby mode**: A toggle switch labeled 'OFF' with an information icon.
- WebSocket passthrough**: A toggle switch labeled 'OFF' with an information icon.

**Figure 304: Add New Path**

3. Click Save.

### Add Exception

(only available for the HTTP based business application rules) This page describes how to specify path exceptions for the web servers.

1. Click Add New Exception.
2. Specify exception details.

#### Path

Specify the path which you want to exclude.

#### Operation

Select the operation among **AND** or **OR** for **Path** and **Source**.

### **Source**

Specify the source networks where the client request comes from and which are to be exempted from the selected check(s).

### **Skip these Checks**

#### **Cookie Signing**

Click to skip cookie signing. Cookie signing protects a web server against manipulated cookies. When the web server sets a cookie, a second cookie is added to the first cookie containing a hash built of the primary cookie's name, its value and a secret, where the secret is only known by the WAF. Thus, if a request cannot provide a correct cookie pair, there has been some sort of manipulation and the cookie will be dropped.

#### **Static URL Hardening**

Protects against URL rewriting. When a client requests a website, all static URLs of the website are signed. The signing uses a similar procedure as with cookie signing. Additionally the response from the web server is analyzed in respect to the links that can be validly requested next.

#### **Form Hardening**

Click to skip form hardening. Form hardening protects against web form rewriting. Form hardening saves the original structure of a web form and signs it. Therefore, if the structure of a form has changed when it is submitted the WAF rejects the request.

#### **Anti-virus**

Select this option to protect a web server against viruses.

#### **Block clients with bad reputation**

Based on GeoIPClosed and RBLClosed information you can block clients which have a bad reputation according to their classification.

### **Skip these categories**

#### **Protocol Violations**

Enforces adherence to the RFC standard specification of the HTTP protocol. Violating these standards usually indicates malicious intent.

#### **Protocol Anomalies**

Searches for common usage patterns. Lack of such patterns often indicates malicious requests. These patterns include, among other things, HTTP headers like 'Host' and 'User-Agent'.

#### **Request Limits**

Enforces reasonable limits on the amount and ranges of request arguments. Overloading request arguments is a typical attack vector.

#### **HTTP Policy**

Narrows down the allowed usage of the HTTP protocol. Web browsers typically use only a limited subset of all possible HTTP options. Disallowing the rarely used options protects against attackers aiming at these often less well supported options.

#### **Bad Robots**

Checks for usage patterns characteristic of bots and crawlers. By denying them access, possible vulnerabilities on your web servers are less likely to be discovered.

#### **Generic Attacks**

Searches for attempted command executions common to most attacks. After having breached a web server, an attacker usually tries to execute commands on the server like expanding privileges or manipulating data stores. By searching for these post-breach execution attempts, attacks can be detected that might otherwise have gone unnoticed, for example because they targeted a vulnerable service by the means of legitimate access.

### **SQL Injection Attacks**

Checks for embedded SQL commands and escape characters in request arguments. Most attacks on web servers target input fields that can be used to direct embedded SQL commands to the database.

### **XSS Attacks**

Checks for embedded script tags and code in request arguments. Typical cross-site scripting attacks aim at injecting script code into input fields on a target web server, often in a legitimate way.

### **Tight Security**

Performs tight security checks on requests, like checking for prohibited path traversal attempts.

### **Trojans**

Checks for usage patterns characteristic of trojans, thus searching for requests indicating trojan activity. It does not, however, prevent the installation of such trojans as this is covered by the antivirus scanners.

### **Outbound**

Prevents web servers from leaking information to the client. This includes, among other things, error messages sent by servers which attackers can use to gather sensitive information or detect specific vulnerabilities.

## **Advanced**

### **Never change HTML during static URL hardening or form hardening**

If selected, no data matching the defined exception settings will be modified by the WAF engine. With this option, e.g., binary data wrongly supplied with a text/html content type by the web server will not be corrupted. On the other hand, web requests may be blocked due to activated URL hardening, HTML rewriting, or form hardening. Those three features use an HTML parser and therefore to some extent depend on the modification of web page content. To prevent undesired blocking, skip URL hardening and/or form hardening for requests affected by blocking; you might need to do this in another/new exception to reflect dependencies between web servers and/or web pages.

### **Accept unhardened form data**

Even though having an exception for form hardening, it is possible that form data will not be accepted if the form hardening signature is missing. With this option, unhardened form data will be accepted anyway.

Path

Search / Add +

Operation

and

▼

Source

Add New Item

Skip these checks

Operation

and

▼

Source

Add New Item

Skip these checks

Cookie Signing

Static URL Hardening

Source

Add New Item

Skip these checks

Cookie Signing

Static URL Hardening

Form Hardening

Anti-virus

Block clients with bad reputation

Skip these categories

Protocol Violations

Protocol Anomalies

Anti-virus

Block clients with bad reputation

Skip these categories

Protocol Violations

Protocol Anomalies

Request Limits

HTTP Policy

3. Click **Save**.

### **Application Protection Templates for common non-HTTP Applications**

SF-OS offers several pre-configured templates to create a protection rule for commonly used non-HTTP applications and services. You can use these templates to create a rule for the web application, that is close to your configuration, then modify it to fit your needs.

Pre-defined templates include:

1. [DNAT/Full NAT/Load Balancing](#)
2. [Mail Servers \(SMTP\)](#)

### **Add DNAT/Full NAT/Load Balancing Rule**

A DNAT/Full NAT/Load Balancing based rule is used to protect non-web servers, like mail or other servers hosted inside the network (LAN or DMZ). Using this rule, you can define access rights of such servers to users who require access over the WAN or Internet.

1. Go to **Protect > Firewall** and select between **IPv4** or **IPv6** using the default filter.
2. Now, click **+Add Firewall Rule** and select **Business Application Rule**.
3. Specify the general rule details.

#### **Application Template**

Select **DNAT/Full NAT/Load Balancing** to configure a rule for generic Non-Web based applications.

#### **Description**

Enter a description for the rule.

#### **Rule Position**

Specify the position of the rule.

**Available Options:** TopBottom

#### **Rule Name**

Specify a name to identify the rule.

Application Template <input type="text" value="DNAT/Full NAT/Load Balancing"/>	Description <input type="text" value="Description"/>	Rule Position <input type="text" value="Top"/>
Rule Name * <input type="text" value="Rule name"/>		

**Figure 306: About This Rule**

4. Specify **Source** details.

#### **Source Zones**

Select a source zone or click **Add New Item** to define a new LAN or DMZ zone.

#### **Allowed Client Networks**

Select the allowed host(s) or add a new one by clicking **Add New Item**.

#### **Blocked Client Networks**

Select the blocked host(s)/network(s).

Source Zones * <input type="text"/>	Allowed Client Networks * <input type="text"/>	Blocked Client Networks <input type="text"/>
<b>Add New Item</b>		<b>Add New Item</b>

**Figure 307: Source**

5. Specify **Destination & Service** details.

## Destination Host/Network

Select the destination host/network to apply rule. It is the public IP address through which users access an internal server/host over the Internet.

**Available Options: IP Address:** Specified IP address is mapped to a corresponding mapped single IP address or a range of IP addresses. If a single IP address is mapped to a range of IP addresses, the device uses a sticky IP algorithm to load balance the requests.**IP Range :** Specified IP address range is mapped to a corresponding range of mapped IP addresses. The IP range defines the start and end of an address range. The start of the range must be lower than the end of the IP. Select when any of the device port, alias or virtual LAN (VLAN) sub-interface is required to be mapped to the destination host or network.

## Services

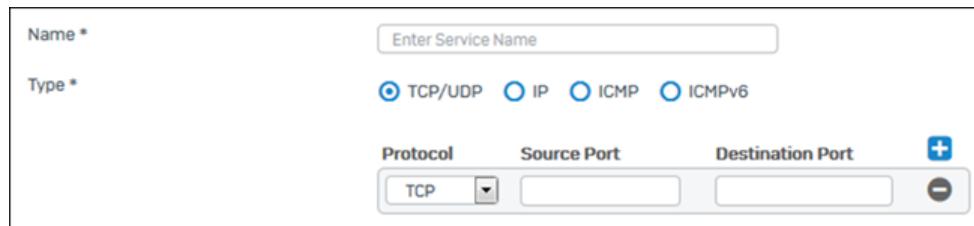
Select the services allowed to the user. You can directly add a new service here.

### Add new item

**Name:** Enter a name to identify the service.

**Type:** Select a protocol for the service.

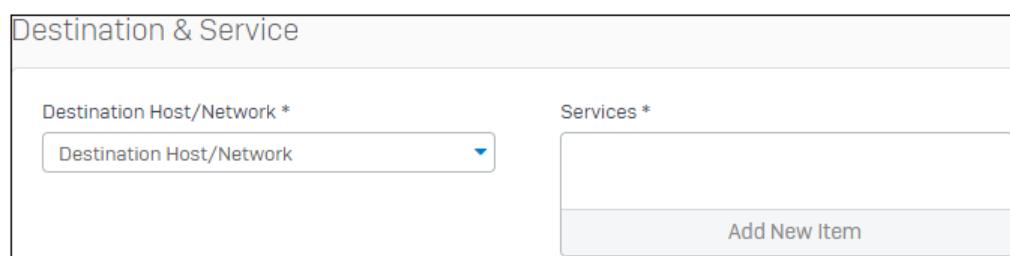
**Available Options:TCP/UDP:** Enter Source and Destination port. You can enter multiple ports for the same service. The number of source and destination ports must not exceed 16.**IP:** Select Protocol Number for the service. You can select multiple ports for the same service.**ICMP:** Select ICMP Type and Code. You can enter multiple types and codes for the same service. Use Add icon  and Remove icon  to add and delete the parameters respectively. **ICMPv6:** Select ICMPv6 Type and Code. You can enter multiple types and codes for the same service. Use Add  and Remove  to add and delete the parameters.



The screenshot shows a configuration form for adding a new service. At the top, there are fields for 'Name \*' and 'Enter Service Name'. Below that, a 'Type \*' field has 'TCP/UDP' selected. Under 'Protocol', 'TCP' is selected. There are fields for 'Source Port' and 'Destination Port', each with a dropdown menu showing 'TCP'. At the bottom right is a blue '+' icon for adding parameters and a grey '-' icon for deleting them.

**Figure 308: Add Service**

## Figure 309: Destination and Service



The screenshot shows a configuration form for destination and services. On the left, there's a dropdown menu for 'Destination Host/Network \*' with 'Destination Host/Network' selected. On the right, there's a large text area labeled 'Services \*' with a 'Add New Item' button at the bottom.

## 6. Specify Forward To details.

### Protected Server(s)

From the available options, select the application servers on which the web server is to be hosted.

Available options: **IP Address:** External IP address is mapped to the specified IP address.**IP Range:** External IP address range is mapped to the specified IP address range.**IP List:** External IP address is mapped to the specified IP list.**FQDN**(available only for IPv4 virtual hosts): External IP address is mapped to the specified FQDN. Internal mapped server can be accessed by FQDN.



**Note:** For **IP Range** and **IP List**, you can also use a single external IP address. The device will then use load balancing for handling the requests.

#### Mapped Port (*available only if Change Destination Port(s) is selected*)

Specify the mapped port number on the destination network to which the public port number is mapped. Mapped port must have the same number of ports as specified in the public service, or at least have one port. **Mapped Port** is disabled if:

- No TCP/UDP service is selected.
- Multiple services are selected.
- Service group is selected.
- Selected service is with TCP/UDP combination.

#### Protected Zone

Select the zone to apply web server rule.

#### Change Destination Port(s)

Select the check box to specify different mapped port. Clear the check box to use the same **Service Port(s) Forwarded** as mapped port.

The screenshot shows a configuration window titled "Forward To". It contains the following fields:

- Protected Server(s) \***: A dropdown menu labeled "Protected Server(s)".
- Mapped Port \***: A field with a "To" button.
- Protected Zone \***: A dropdown menu labeled "Protected Zone".
- Change Destination Port(s)**: A checkbox labeled "Change Destination Port(s)".

**Figure 310: Forward To**

#### 7. Specify Load balancing details.

#### Load Balancing (*available only if selected Protected Server is IP Range or IP List or selected Destination Host/Network is IP Address*)

Select the method for load balancing from the available options.

Available Options:**Round Robin**: In this method, requests are served in a sequential manner where the first request is forwarded to the first server, second request to the second server and so on. When a request is received, the device checks to see which was the last server that was assigned a request. It then assigns this new request to the next available server. This method can be used when equal distribution of traffic is required and there is no need for session-persistence.**First Alive**: In this method, all incoming requests are served by the first server (the first IP address that is configured in the IP range). This server is considered as the primary server and all others are considered as backup. Only when the first server fails, the requests are forwarded to the next server in line. This method is used for failover scenarios. **Random**: In this method, the requests are forwarded to the servers randomly. Nevertheless, the device makes sure that all configured servers receive equally distributed load. Hence, this method is also called uniform random distribution. This method can be used when equal distribution of traffic is required and there is no need for session-persistence or order of distribution.**Sticky IP**: In this method, along with the Round Robin distribution of traffic, the device forwards incoming traffic according to the combination of source and destination IP address. All traffic from a particular source is forwarded only to its mapped server. This means that all requests for a given source IP are sent to the same application server instance. This method is useful in cases where all requests or sessions are required to be processed by the same server. For example: banking websites, E-Commerce websites.

#### Health Check (*available only if Load Balancing is enabled*)

Click to enable a health check for failover and specify the parameters based on the description shown below.

#### **Port (available only if selected Health Check Method is TCP Probe)**

Specify the port number on the server health is monitored.

Acceptable range: 1 to 65535

#### **Interval**

Specify the time interval in seconds after which the health will be monitored.

Acceptable range: 5 to 65535 seconds

Default: 60

#### **Probe Method**

Select the probe method to check the health of the server from the available options.

**Available Options:** ICMP TCP

#### **Timeout**

Specify the time interval in seconds within which the server must respond.

Acceptable range: 1 to 10 seconds

Default: 2

#### **Retries**

Specify the number of tries to probe the health of the server, after which the server will be declared unreachable.

Acceptable range: 1 to 10

Default: 3

<b>Load Balancing</b> <input type="checkbox" value="Sticky IP"/> Sticky IP <input checked="" type="checkbox"/> Health Check <b>Probe Method</b> <input type="checkbox" value="TCP"/> TCP	<b>Port</b> <input type="text"/> <b>Interval(Seconds)</b> <input type="text" value="60"/> <b>Timeout</b> <input type="text" value="2"/> <b>Retries</b> <input type="text" value="3"/>
--	--

**Figure 311: Load Balancing**

- Specify **Identity** details.

#### **Match known users**

Match rule based on user identity allows you to check whether the specified user/user group from the selected zone is allowed to access the selected service or not.

Click to attach the user identity.

Enable **check identity** to apply the following policies per user.

#### **Show Captive Portal to unknown users**

Select the check box to accept traffic from unknown users. Captive portal page is displayed to the user where the user can login to access the Internet.

Clear the check box to drop traffic from unknown users.

#### User or Groups (*available if Match known users is selected*)

Select the user(s) or group(s) from the list of available options.

#### Exclude this user activity from data accounting (*available if Match known users is selected*)

Click to enable/disable user traffic activity from data accounting.

By default, user's network traffic is considered in data accounting. Select to exclude certain traffic from user data accounting. The traffic allowed through this firewall rule will not be accounted towards data transfer for the user.

The screenshot shows the 'Identity' configuration section. On the left, there are two checkboxes: 'Match known users' (checked) and 'Show captive portal to unknown users' (unchecked). To the right, there is a 'User or Groups' section with a list box labeled 'User or Groups' and a button 'Add New Item'. At the bottom, there is a checkbox 'Exclude this user activity from data accounting' (unchecked).

**Figure 312: Identity**

#### 9. Specify Advanced settings details.

##### a) Specify Policies for Business Applications.

###### Intrusion Prevention

Select the required IPS policy. If **Match rule based on user identity** is enabled, user's IPS policy will be applied automatically, but will not be effective till the respective module is subscribed. A new IPS policy can be created directly from this page or from the **Protect > Intrusion Prevention > IPS Policies** page.

###### Traffic Shaping Policy

Select the required traffic shaping policy. If **Match rule based on user identity** is enabled, user's traffic shaping policy will be applied automatically.

You need to select traffic shaping policy for the rule if **Match known users** is not selected.

A new traffic shaping policy can be created directly from this page or from the **System > Profiles > Traffic Shaping** page.

The screenshot shows the 'Policies for Business Applications' configuration page. It has two dropdown menus: 'Intrusion Prevention' (set to 'None') and 'Traffic Shaping' (set to 'User's policy applied').

**Figure 313: Policies for Business Applications**

##### b) Specify Security Heartbeat details (*available only if IPv4 is selected*).

###### Minimum Source HB Permitted

Select a minimum health status that a source device must have to conform to this rule. Health status can be either **Green**, **Yellow** or **No Restriction**. If the health criterion is not met, access and privileges defined in this rule will not be granted to the user.

### Block clients with no heartbeat

Heartbeat-capable devices can be required to send information on their health status in defined intervals - this is called a heartbeat.

Based on that information, you can restrict a source device's access to certain services and networks.

Enable the option to require the sending of heartbeats.

### Block request to destination with no heartbeat (*not available if Protected Zone selected is WAN*)

Heartbeat-capable devices can be required to send information on their health status in defined intervals - this is called a heartbeat.

Based on that information, you can block requests to destinations not sending heartbeat.

Enable/disable the option to require the sending of heartbeats.

<b>Minimum Source HB Permitted:</b>		
<input type="radio"/> GREEN	<input type="radio"/> YELLOW	<input checked="" type="radio"/> No Restriction
<input type="checkbox"/> Block clients with no heartbeat		
<b>Minimum Destination HB Permitted:</b>		
<input type="radio"/> GREEN	<input type="radio"/> YELLOW	<input checked="" type="radio"/> No Restriction
<input type="checkbox"/> Block request to destination with no heartbeat		

**Figure 314: Synchronized Security**

- c) Specify **Routing** details.

#### Rewrite source address (Masquerading)

Enable/disable to re-write the source address or specify a NAT policy.

#### Use Outbound Address (*available only if Rewrite source address is enabled*)

Select the NAT policy to be applied from the list of available NAT policies.

A new NAT policy can be created directly from this page or from the **System > Profiles > Network Address Translation** page.

The default NAT policy is **Masquerade**.

**MASQ (Interface Default IP):** IP Address of the selected Protected Zone as configured in **Configure > Network > Interfaces** will be displayed instead of (Interface Default IP).

#### Create Reflexive Rule

Enable to automatically create a reflexive firewall rule for the protected host.

A reflexive rule has the same policies as those rules configured for the hosted server but instead of source zone to destination zone, this rule is applicable on traffic from destination zone to source zone.

By default, the reflexive rule is not created.

**Figure 315: Routing**

10. Specify the logging option for the user application traffic.

#### **Log Firewall Traffic**

Click to enable logging of permitted and denied traffic.

**Figure 316: Log Traffic**

11. Click Save.

The non-web based rule has been created and appears on the **Firewall** page when the appropriate filter is set.

#### **Add Rule for Email Clients (POP and IMAP)**

Email Clients (POP and IMAP) rule is used to protect mail servers which are hosted publicly (WAN). This page describes how to configure a protection rule and control access of mail servers using application template - Email Clients .



#### **Note:**

If you delete Email Clients rule, the Emails which are under process by this rule will be queued but will not be delivered.

We recommend to follow below given steps so that you do not lose all the emails processed by this rule:

1. Before deleting this rule, clone this rule by choosing **Clone Above** option and change the **Action** to **Drop**. This cloned rule will hold all the incoming emails.
  2. Go to **Email > Mail Spool** and check if spool is empty.
  3. Once the spool is empty, delete both the firewall rules.
1. Go to **Protect > Firewall** and select between **IPv4** or **IPv6** using the default filter.
  2. Now, click **+Add Firewall Rule** and select **Business Application Rule**.
  3. Specify the general rule details.

#### **Application Template**

Select **Email Clients (POP & IMAP)** to define a application filter policy for POP and IMAP based email clients.

#### **Description**

Specify the rule description.

#### **Rule Position**

Specify the position of the rule.

**Available Options:** TopBottom

#### **Rule Name**

Specify a name to identify the rule.

Application Template <input type="text" value="Email Clients(POP &amp; IMAP)"/>	Description <input type="text" value="Allows scanning of POP3/IMAP client traffic by Email Scanning Rules."/>	Rule Position <input type="text" value="Top"/>
Rule Name * <input type="text" value="Rule name"/>		

**Figure 317: About This Rule**

4. Specify **Source** details.

**Zone**

Select the allowed source zone(s).

**Networks**

Select the allowed source network(s). A new network host can be created directly from this page or from the **System > Hosts and Services > IP Host** page.

<b>Zone *</b> <input type="text"/> <input type="button" value="Add New Item"/>	<b>Networks *</b> <input type="text"/> <input type="button" value="Add New Item"/>
--	--

**Figure 318: Source**

5. Specify **Destination** details.

**Zone**

Select the zone to which the rule applies.

**Networks**

Select the network(s) to be protected.

A new network host can be created directly from this page or from the **System > Hosts and Services > IP Host** page.

<b>Zone *</b> <input type="text"/> <input type="button" value="Add New Item"/>	<b>Networks *</b> <input type="text"/> <input type="button" value="Add New Item"/>
--	--

**Figure 319: Destination**

6. Specify **Identity** details.

**Match rule based on user identity**

Click to enable a rule based on the user identity.

**Show Captive Portal to unknown users**

Select the check box to accept traffic from unknown users. Captive portal page is displayed to the user where the user can login to access the Internet.

Clear the check box to drop traffic from unknown users.

**User or Groups (available only if Match rule based on user identity is enabled)**

Select the user(s) or group(s) from the list of available options.

**Exclude this user activity from data accounting (only available if Match rule based on user identity is enabled)**

Click to enable/disable user traffic activity from data accounting.

By default, user's network traffic is considered in data accounting. Select to exclude certain traffic from user data accounting. The traffic allowed through this rule will not be accounted towards data transfer for the user.

The screenshot shows a configuration interface for 'Identity'. On the left, there are two checkboxes: one checked for 'Match known users' and one unchecked for 'Show captive portal to unknown users'. To the right is a section titled 'User or Groups' containing a large empty text input field and a 'Add New Item' button. At the bottom right is another checkbox labeled 'Exclude this user activity from data accounting'.

**Figure 320: Identity**

**7. Specify Malware Scanning details.**

**Scan IMAP/IMAPS/POP3/POP3S/SMTP/SMTPTS**

Click to enable/disable scanning of IMAP/IMAPS/POP3/POP3S/SMTP/SMTPTS traffic.

The screenshot shows a grid of six checkboxes for scanning different protocols. The first row contains 'Scan IMAP' (checked), 'Scan POP3' (checked), and 'Scan SMTP' (unchecked). The second row contains 'Scan IMAPS' (checked), 'Scan POP3S' (checked), and 'Scan SMTPTS' (unchecked). Each checkbox has a small orange warning icon next to it.

**Figure 321: Malware Scanning**

**8. Specify Advanced settings.**

a) **Specify Policies for Business Applications.**

**Intrusion Prevention**

Select an IPS policy for the rule. A new IPS policy can be created directly from this page itself or from the **Protect > Intrusion Prevention > IPS Policies** page.

**Traffic Shaping (Not available if Match rule based on user identity is selected)**

Select a traffic shaping policy for the rule.

A traffic shaping policy allocates & limits the maximum bandwidth usage of the user.

A new traffic shaping policy can be created directly from this page or from the **System > Profiles > Traffic Shaping** page.

The screenshot shows a configuration interface for 'Policies for Business Applications'. It features two dropdown menus. The top menu is labeled 'Intrusion Prevention' and has 'None' selected. The bottom menu is labeled 'Traffic Shaping' and also has 'None' selected.

**Figure 322: Policies for Business Applications**

b) **Specify Security Heartbeat settings (available only if IPv4 is selected).**

**Minimum Source HB Permitted**

Select a minimum health status that a source device must have to conform to this rule. Health status can be either **Green**, **Yellow** or **No Restriction**. If the health criterion is not met, access and privileges defined in this rule will not be granted to the user.

#### **Block clients with no heartbeat**

Heartbeat-capable devices can be required to send information on their health status in defined intervals - this is called a heartbeat.

Based on that information, you can restrict a source device's access to certain services and networks.

Enable/disable the option to require the sending of heartbeats.

#### **Minimum Destination HB Permitted (Not available if the only Destination Zone selected is WAN)**

Select a minimum health status that a destination device must have to conform to this rule. Health status can be either **Green**, **Yellow** or **No Restriction**. If the health criterion is not met, access and privileges defined in this policy will not be granted to the user.

 **Note:** You can use the option if you have selected multiple zones along with WAN.

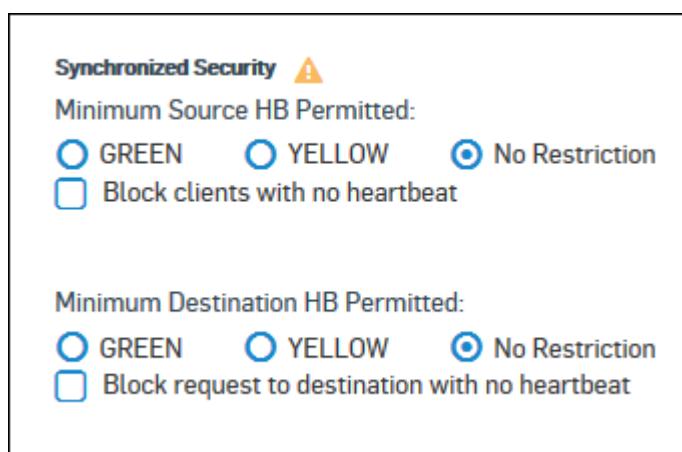
#### **Block request to destination with no heartbeat (Not available if the only Destination Zone selected is WAN)**

Heartbeat-capable devices can be required to send information on their health status in defined intervals - this is called a heartbeat.

Based on that information, you can block requests to destinations not sending heartbeat.

Enable/disable the option to require the sending of heartbeats.

 **Note:** You can use the option if you have selected multiple zones along with WAN.



**Figure 323: Security Heartbeat**

- Specify **Routing** details.

#### **Rewrite source address (Masquerading)**

Enable/disable to re-write the source address or specify a NAT policy.

#### **Use Gateway Specific Default NAT Policy (*only if Masquerading is selected*)**

Select to override the default NAT policy with a gateway specific policy.

#### **Override default NAT policy for specific Gateway (*only if Use Gateway Specific Default NAT Policy is selected*)**

Select to specify gateway and corresponding NAT policy. Multiple gateways and NAT policies can be added.

#### **Use Outbound Address (*available only if Rewrite source address is enabled and Use Gateway Specific Default NAT Policy is disabled*)**

Select the NAT policy to be applied the list or available NAT policies.

A new NAT policy can be created directly from this page or from the **System > Profiles > Network Address Translation** page.

The default NAT policy is **Masquerade**.

#### MASQ (Interface Default IP)

- IP Address of the Destination Zone as configured in **Configure > Network > Interfaces** will be displayed instead of (Interface Default IP) when single **Destination Zone** is selected.
- (Interface Default IP) will be displayed when multiple **Destination Zones** are selected.

#### Primary Gateway

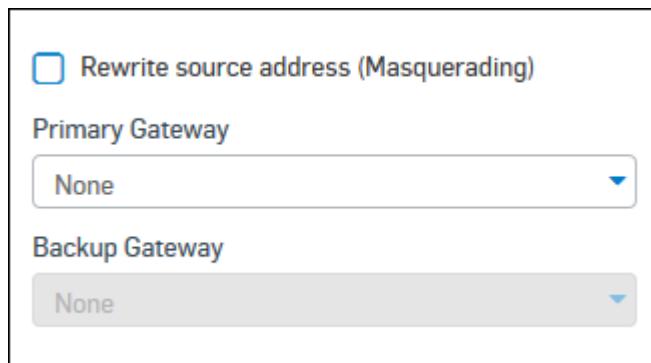
Select the primary gateway to route the request. You can create new gateway from this page itself or from **Configure > Routing > Gateways**.

 **Note:** On deletion of the gateway, **Primary Gateway** will display **WAN Link Load Balance** for WAN Destination Zone and **None** for other zones. In such case, firewall rule will not make routing decisions.

#### Backup Gateway

Select the backup gateway to route the request. You can create new gateway from this page itself or from **Configure > Routing > Gateways**.

 **Note:** On deletion of the gateway, **Backup Gateway** will display **None**.



The screenshot shows a configuration window for routing. It includes a checkbox for "Rewrite source address (Masquerading)". Below it are two dropdown menus: "Primary Gateway" set to "None" and "Backup Gateway" also set to "None".

**Figure 324: Routing**

- Specify logging option for the user application traffic.

#### Log Firewall Traffic

Click to enable logging of permitted and denied traffic.



The screenshot shows a configuration window for log traffic. It contains a single checkbox labeled "Log Firewall Traffic".

**Figure 325: Log Traffic**

#### Add Rule for Email Servers (SMTP)

This page describes how to configure a rule for email servers (SMTP).

- Go to **Protect > Firewall** and select between **IPv4** or **IPv6** using the default filter.
- Now, click **+Add Firewall Rule** and select **Business Application Rule**.
- Specify the general rule details.

#### Application Template

Select **Email Servers (SMTP)** to configure a rule for SMTP based email applications.

#### Description

Specify the policy description.

#### Rule Position

Specify the position of the rule.

**Available Options:** TopBottom

#### Rule Name

Specify a name to identify the policy.

Application Template <input type="button" value="Email Servers(SMTP)"/>	Description Allows routing of SMTP traffic to Email server for scanning by Email Scanning Rules.	Rule Position <input type="button" value="Top"/>
Rule Name * <input type="text" value="Rule name"/>		

**Figure 326: About This Rule**

4. Specify **Source** details.

#### Source Zones

Click to select the source zone. Click **Add New Item** to define a new LAN or DMZ zone.

#### Allowed Client Networks

Select the allowed host(s) or add a new one by clicking **Add New Item**.

#### Blocked Client Networks

Select the blocked host(s)/network(s).

Source Zones * <input type="button" value="Add New Item"/>	Allowed Client Networks * <input type="button" value="Add New Item"/>	Blocked Client Networks <input type="button" value="Add New Item"/>
---	--	--

**Figure 327: Source**

5. Specify **Destination & Service** details.

#### Destination Host/Network

Select the destination host/network to apply rule. It is the public IP address through which users access internal server/host over the Internet.

**Available Options:IP Address** – Specified IP address is mapped to a corresponding mapped single or range of IP addresses. If a single IP address is mapped to a range of IP addresses, the device uses a sticky IP algorithm to load balance the requests.**IP Range** – Specified IP address range is mapped to a corresponding range of mapped IP addresses. The IP range defines the start and end of an address range. The start of the range must be lower than the end of the range.**Interface IP (only available for IPv4)** – Select when any of the device port, alias or virtual LAN (VLAN) sub interface is required to be mapped to the destination host or network.

#### Services

Select the services allowed to the user. A new service can be directly created from this page.

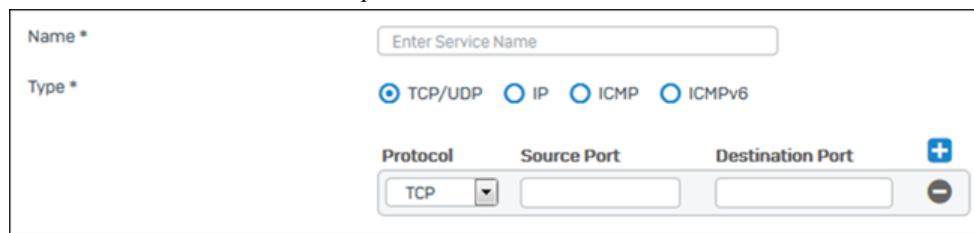
##### Add new item

**Name:** Enter a name to identify the service.

**Type:** Select a protocol for the service.

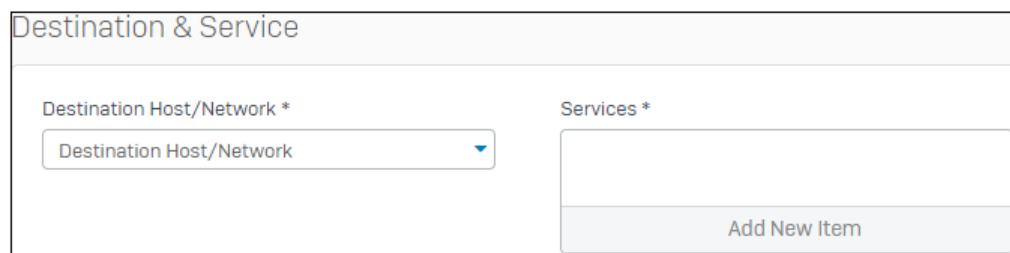
**Available Options:TCP/UDP:** Enter Source and Destination port. You can enter multiple ports for the same service. The number of source and destination ports must not exceed 16.**IP:** Select Protocol Number for the service. You can select multiple ports for the same service.**ICMP:** Select ICMP Type and Code. You can enter multiple types and codes for the same service. Use Add icon  and Remove icon  to add and delete the parameters respectively. **ICMPv6:** Select ICMPv6

Type and Code. You can enter multiple types and codes for the same service. Use Add  and Remove  to add and delete the parameters.



**Figure 328: Add Service**

**Figure 329: Destination and Service**



## 6. Specify **Forward To** details.

### Protected Server(s)

Select from the available options on which the email server is to be hosted.

**Available options:** **IP Address** – External IP address is mapped to the specified IP address.**IP Range** – External IP address range is mapped to the specified IP address range.**IP List** – External IP address is mapped to the specified IP list.**FQDN** (*available only for IPv4 virtual hosts*) – External IP address is mapped to the specified FQDN. Internal mapped server can be accessed by FQDN.

 **Note:** For **IP Range** and **IP List**, you can also use a single external IP address. The device will then use load balancing for handling the requests.

### Mapped Port (*available only if Change Destination Port(s) is selected*)

Specify mapped port number on the destination network to which the public port number is mapped. Mapped port must have the same number of ports as specified in the public service, or at least have one port. **Mapped Port** is disabled if:

- No TCP/UDP service is selected.
- Multiple services are selected.
- Service group is selected.
- Selected service is with TCP/UDP combination.

### Protected Zone

Select the zone to which the email server rule applies.

### Change Destination Port(s)

Select the check box to specify different mapped port. Clear the check box to use the same **Service Port(s) Forwarded** as mapped port.

The screenshot shows a configuration interface titled 'Forward To'. It includes fields for 'Protected Server(s)' (with a dropdown menu), 'Mapped Port' (with a 'To' field), 'Protected Zone' (with a dropdown menu), and a checkbox for 'Change Destination Port(s)'. The entire interface is contained within a light gray border.

**Figure 330: Forward To**

7. Specify Load balancing details.

**Load Balancing (available only if selected Protected Server is IP Range or IP List and selected Destination Host/Network is IP Address)**

Select the method for load balancing from the available options.

Available Options:**Round Robin** - In this method, requests are served in a sequential manner where the first request is forwarded to the first server, second request to the second server and so on. When a request is received, the device checks to see which the last server that was assigned a request was. It then assigns this new request to the next available server. This method is can be used when equal distribution of traffic is required and there is no need for session-persistence.**First Alive** - In this method, all incoming requests are served by the first server (the first IP address that is configured in the IP range). This server is considered as the primary server and all others are considered as backup. Only when the first server fails, the requests are forwarded to the next server in line. This method is used for failover scenarios. **Random** -In this method, the requests are forwarded to the servers randomly. Although, the device makes sure that all configured servers receive equally distributed load. Hence, this method is also called uniform random distribution. This method can be used when equal distribution of traffic is required and there is no need for session-persistence or order of distribution.**Sticky IP** - In this method, along with Round Robin distribution of traffic, the device forwards incoming traffic according to the combination of source and destination IP address. All traffic from a particular source is forwarded only to its mapped server. This means that all requests for a given source IP are sent to the same application server instance. This method is useful in cases where all requests or sessions are required to be processed by the same server. For example: Banking websites, E-Commerce websites.

**Health Check (available only if Load Balancing is enabled)**

Click to enable health check for failover and specify the parameters based on the description shown below.

**Port (available only if selected health check method is TCP Probe)**

Specify the port number on the server health is monitored.

Acceptable range: 1 to 65535

**Interval**

Specify the time interval in seconds after which the health will be monitored.

Acceptable range: 5 to 65535 seconds

Default: 60

**Probe Method**

Select the probe method to check the health of the server from the available options.

Available Options:ICMP TCP

**Timeout**

Specify the time interval in seconds within which the server must respond.

Acceptable range: 1 to 10 seconds

Default: 2

#### Retries

Specify the number of tries to probe the health of the server, after which the server will be declared unreachable

Acceptable range: 1 to 10

Default: 3

Load Balancing	Port
Sticky IP	
<input checked="" type="checkbox"/> Health Check	Interval(Seconds)
TCP	60
Probe Method	Timeout
	2
	Retries
	3

**Figure 331: Load Balancing**

- Specify Identity details.

#### Match known users

**Match known users** allows you to check whether the specified user/user group from the selected zone is allowed to access the selected service or not.

Click to attach the user identity.

#### Show Captive Portal to unknown users

Select the check box to accept traffic from unknown users. Captive portal page is displayed to the user where the user can login to access the Internet.

Clear the check box to drop traffic from unknown users.

#### User or Groups (*available only if Match known users is enabled*)

Select the user(s) or group(s) from the list of available options.

#### Exclude this user activity from data accounting (*available only if Match known users is enabled*)

Click to enable/disable user traffic activity from data accounting.

By default, user's network traffic is considered in data accounting. Select to exclude certain traffic from user data accounting. The traffic allowed through this firewall rule will not be accounted towards data transfer for the user.

<input checked="" type="checkbox"/> Match known users	User or Groups
<input type="checkbox"/> Show captive portal to unknown users	Add New Item
<input type="checkbox"/> Exclude this user activity from data accounting	

**Figure 332: Identity**

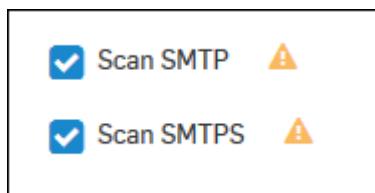
9. Specify **Scanning** details.

**Scan SMTP**

Click to enable/disable scanning of SMTP traffic.

**Scan SMTPTS**

Click to enable/disable scanning of SMTPTS traffic.



**Figure 333: Scanning**

10. Specify **Advanced** settings details.

a) Specify **Polices for Business Applications**.

**Intrusion Prevention**

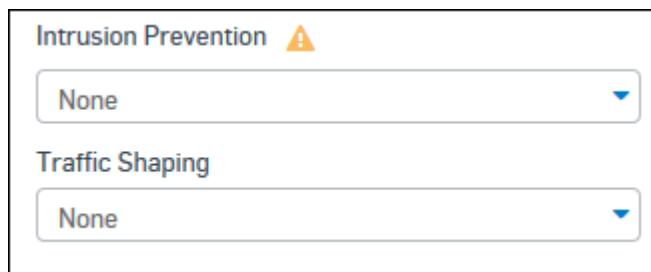
Select the required IPS policy. If **Match rule based on user identity** is enabled, user's IPS policy will be applied automatically, but will not be effective till the respective module is subscribed.

A new IPS policy can be created directly from this page or from the **Protect > Intrusion Prevention > IPS Policies** page.

**Traffic Shaping Policy (not available if Match known users is selected)**

Select the required QoS policy. If **Match rule based on user identity** is enabled, user's QoS policy will be applied automatically.

A new traffic shaping policy can be created directly from this page or from the **System > Profiles > Traffic Shaping** page.



**Figure 334: Policies for Business Applications**

b) Specify **Security Heartbeat** settings (*available only if IPv4 is selected*).

**Minimum Source HB Permitted**

Select a minimum health status that a source device must have to conform to this rule. Health status can be either **Green**, **Yellow** or **No Restriction**. If the health criterion is not met, access and privileges defined in this rule will not be granted to the user.

**Block clients with no heartbeat**

Heartbeat-capable devices can be required to send information on their health status in defined intervals - this is called a heartbeat.

Based on that information, you can restrict a source device's access to certain services and networks.

Enable/disable the option to require the sending of heartbeats.

**Minimum Destination HB Permitted (not available if Protected Zone selected is WAN)**

Select a minimum health status that a destination device must have to conform to this rule. Health status can be either **Green**, **Yellow** or **No Restriction**. If the health criterion is not met, access and privileges defined in this rule will not be granted to the user.

### Block request to destination with no heartbeat (*not available if Protected Zone selected is WAN*)

Heartbeat-capable devices can be required to send information on their health status in defined intervals - this is called a heartbeat.

Based on that information, you can block requests to destinations not sending heartbeat.

Enable/disable the option to require the sending of heartbeats.

The screenshot shows the 'Synchronized Security' configuration section. It includes two sets of options:

- Minimum Source HB Permitted:**
  - GREEN
  - YELLOW
  - No Restriction
  - Block clients with no heartbeat
- Minimum Destination HB Permitted:**
  - GREEN
  - YELLOW
  - No Restriction
  - Block request to destination with no heartbeat

**Figure 335: Security Heartbeat**

- c) Specify **Routing** details.

#### Rewrite source address (Masquerading)

Enable/disable to re-write the source address or specify a NAT policy.

#### Use Outbound Address (*available only if Rewrite source address is enabled*)

Select the NAT policy to be applied from the list of available NAT policies.

A new NAT policy can be created directly from this page or from the **System > Profiles > Network Address Translation** page.

The default NAT policy is **Masquerade**.

**MASQ (Interface Default IP):** IP Address of the selected Protected Zone as configured in **Configure > Network > Interfaces** will be displayed instead of (Interface Default IP).

#### Create Reflexive Rule

Select ON to automatically create a reflexive firewall rule for the protected host.

The reflexive rule has the same policies as those configured for the hosted server but instead of source zone to destination zone, this rule is applicable on traffic from destination zone to source zone.

By default, the reflexive rule is not created.

The screenshot shows the 'Routing' configuration section. It includes the following options:

- Rewrite source address [Masquerading]
- Use Outbound Address** dropdown menu set to **MASQ**
- Create Reflexive Rule

**Figure 336: Routing**

11. Specify the logging option for the user application traffic.

#### Log Firewall Traffic

Click to enable logging of permitted and denied traffic.

<input type="checkbox"/>	Log Firewall Traffic
--------------------------	----------------------

**Figure 337: Log Traffic**

#### Related information

[Protect Internal Email Server - Legacy Mode](#)

## Intrusion Prevention

---

This section covers the following topics:

- [DoS Attacks](#) : Provides information about DoS attacks.
- [IPS Policies](#) : Allows you to configure IPS policies.
- [Custom IPS Signatures](#) : Allows you to add custom IPS signatures.
- [DoS & Spoof Protection](#) : Allows you to configure DoS settings to identify DoS attacks.

### DoS Attacks

The page provides information about DoS attacks. The list shows:

#### Attack Type

Displays the attack type: SYN Flood, UDP Flood, TCP Flood, ICMP Flood and IP Flood.

#### Source

Displays whether source packet control is applied or not. If applied, it indicates the number of packets dropped.

#### Destination

Displays whether destination packet control is applied or not. If applied, it indicates the number of packets dropped.

Click the name of the attack type you want to view to get real time updates on flooding.

Attack Type	Source		Destination	
	Applied	Traffic Dropped	Applied	Traffic Dropped
SYN Flood	No	0	No	0
UDP Flood	No	0	No	0
TCP Flood	No	0	No	0
ICMP Flood	No	0	No	0
IP Flood	No	0	No	0

**Figure 338: DoS Attacks**

### IPS Policies

This page displays the list of all the pre-defined and custom IPS policies.

The device is a real time Intrusion Prevention System (IPS) system that protects your network from known and unknown attacks by worms and viruses, hackers and other Internet risks.

The device at the perimeter of your network analyzes entire traffic and prevents attacks from reaching your network. Whether it is a worm, a suspicious web request, a hacker targeting your mail server or any other attack - it simply does not get through.



**Note:** Intrusion Prevention System module is a subscription module that needs to be subscribed before use.



**Note:** You can also view and manage the IPS status on the **Monitor & Analyze > Diagnostics > Services** page.

IPS consists of a signature engine with a predefined set of signatures. Signatures are the patterns that are known to be harmful. IPS compares traffic to these signatures and responds at a high rate of speed if it finds a match. Signatures included within the device are not editable.

As per your network requirements, device allows you to define multiple policies instead of one global policy, to decrease packet latency and reduce the false positives.

IPS policy allows you to view predefined signatures and customize the intrusion prevention configuration at the category as well as individual signature level. Categories are signatures grouped together based on the application and protocol vulnerabilities.

The device instead of providing only a single policy (global) for managing multiple networks/hosts, allows to tailor policy per network/host i.e. allows to define multiple policies for managing multiple networks/hosts.

To enable the Intrusion Prevention System, apply IPS policy from Security Policies. You can create rule to apply:

- single policy for all the users/networks
- different policies for different users/networks or hosts

As Security Policies control all traffic passing through the device and decide whether to allow or drop the connection, IPS rule will be applied to only that traffic/packet which passes through Firewall.

### Category

Signatures are organized in categories such as DNS, Finger, P2P, DDOS, and others. These signature categories are listed in the policy. You can configure these categories to change the prevention and/or detection settings. To perform Intrusion Prevention, you need to enable IPS services for each category i.e. you will be able to configure attack threats for individual signature only if an IPS service for the category is “Enabled”.

Each IPS policy contains a set of signatures that device searches for, logs, blocks and allows to:

- Enable or disable category from IPS protection.
- Enable or disable individual signature in a category to tailor IPS protection based on your network environment.
- Define an action to be taken when the matching traffic pattern is found. Device can either detect or drop the connection. In either of the case, device generates the log and alerts the Network Administrator.

IPS provides six actions for managing attack threats: (action if signature matches)

- **Allow Packet** - Allows the packet to its intended destination.
- **Drop Packet** - Drops packets if detects any traffic that matches the signature.
- **Disable** - Disables the signature, if it detects any traffic that matches the signature.
- **Drop Session** - Drops the entire session if detects any traffic that matches the signature.
- **Reset** - Resets entire session if detects any traffic that matches the signature.
- **Bypass Session** - Allows the entire session if detects any traffic that matches the signature.

In packet-based actions, the device checks each packet before taking an action while for session-based action, only the first packet is checked and an action is taken. In case of Reset, TCP reset packet is sent to the originator. In all the cases, the device generates the log and alerts the Network Administrator.

To save resources and avoid latency, set action as “Bypass Session” as in this, if the initial packets match the signature then the rest of the session packets will not be scanned at all.

To avoid getting high number of Alerts and save resources, set action as “Drop session” as in this, if the device identifies attack in the initial packets then it will terminate the entire session instead of scanning all the session packets.

The page provides option to add a new policy, configure the handling of signatures by category or on a signature-by-signature basis, or delete the policy.

The device provides following pre-defined policies. You can directly use policies 1 to 6 without any modifications while policies 7 to 10 can either be used directly or, can be modified as per your requirements:

1. DMZ TO LAN
2. DMZ TO WAN
3. LAN TO DMZ
4. LAN TO WAN
5. WAN TO DMZ
6. WAN TO LAN
7. generalpolicy
8. lantowan strict policy
9. lantowan general policy
10. dmzpolicy

### Create IPS Policy

This page describes how to quickly configure a new IPS policy.

1. Go to **Protect > Intrusion Prevention > IPS Policies** and click **Add**.
2. Enter a unique name for the IPS policy.
3. Enter a description for the IPS policy.
4. Select the IPS policy to be used as a template from the list.

The screenshot shows a modal dialog box for creating an IPS policy. It has three input fields: 'Name \*' (with a red asterisk indicating it's required), 'Description', and 'Clone Rules' (with a dropdown menu labeled 'Select Policy'). At the bottom are two buttons: a blue 'Save' button and a white 'Cancel' button.

**Figure 339: Details**

5. Click **Save**.

Once the policy is created, policy rules can be added to take appropriate action for signatures in the policy. Define a rule to configure an action to be taken when the matching traffic pattern is found. If the rules are already added, a list of rules is displayed along with its details like signature filtering criteria, action.

### IPS Policy Rules

Once the policy is created, policy rules can be added to take appropriate action for signatures in the policy. Define a rule to configure an action to be taken when the matching traffic pattern is found. If the rules are already added, a list of rules is displayed along with its details like signature filtering criteria, action.

1. Go to **Protect > Intrusion Prevention > IPS Policies**.
2. Click on the icon under the Manage column for the IPS policy for which you want to add the policy rule.
3. Click **Add**.
4. Enter a unique name for the IPS policy rule.

Rule Name *	<input type="text"/>
-------------	----------------------

**Figure 340: Rule Detail**

5. Enter the Signature Criteria.

**Default**

Select to view a list of default signatures.

**Custom Signature**

Select to view a list of custom signatures.

**Category**

Select IPS signature category from the list of available categories.

**Severity**

Severity is the level of threat posed by the attack. Select the type of severity from the available options.

Available Options:

- Select All
- 1 - Critical
- 2 - Major
- 3 - Moderate
- 4 - Minor
- 5 - Warning

**Platform**

Platform is the OS affected by the attack. Select the platform from the available options:

Available Options:

- Select All
- Windows
- Linux
- Unix
- MAC
- Solaris
- BSD
- Other

**Target**

Target is the type of device targeted by the attack. Select the target from available options:

Available Options:

- Select All
- Client
- Server

**Smart Filter (*available only if Select All is selected*)**

Enter the partial or full signature name to filter by name.



**Figure 341: Signature Criteria**

- Manage the list of Matching Signatures.

#### Select All

Select to choose all the signatures listed for the selected criteria.

Based on the signature criteria the signatures are made available.

#### Select Individual Signature

Select to customize the choice of signatures list for the selected criteria.

Based on the signature criteria the signatures are made available.

**Note:** You can filter the list based on Name and SID, only if you have selected the option Select Individual Signature.

<input type="radio"/> Select All	<input type="radio"/> Select Individual Signature	Name	SID	Category	Severity	Platform	Target	Recommended Action
<input checked="" type="checkbox"/>		Microsoft Word RTF listoverridecount Memory Corruption	1140324042	Office Tools	1 - Critical	Windows	Client	Drop Packet
<input checked="" type="checkbox"/>		Microsoft Word RTF listoverridecount Memory Corruption	1140324040	Office Tools	1 - Critical	Windows	Client	Drop Packet
<input checked="" type="checkbox"/>		Microsoft Word RTF listoverridecount Memory Corruption	1140324041	Office Tools	1 - Critical	Windows	Client	Drop Packet
<input checked="" type="checkbox"/>		"FILE-FLASH Adobe Flash Player DisplayObject use after free attempt"	43410	Multimedia	1 - Critical	Windows	Client	Drop Packet
<input checked="" type="checkbox"/>		"FILE-FLASH Adobe Flash Player DisplayObject use after free attempt"	43412	Multimedia	1 - Critical	Windows	Client	Drop Packet

**Figure 342: List of Matching Signatures**

- Specify the Action details.

#### Action

Select an action to be taken from the available options:

Available Options:**Recommended:** This action means that you want the OS to handle this alert level according to best-fit recommendations.**Allow Packet:** Allows the packet to its intended destination.**Drop Packet:** Drops packets if it detects any traffic that matches the signature. **Disable:** Disables the signature, if it detects any traffic that matches the signature. **Drop Session:** Drops the entire session if detects any traffic that matches the signature. **Reset:** Resets entire session if detects any traffic that matches the signature.**Bypass Session:** Allows the entire session if detects any traffic that matches the signature.

Action	Drop Packet	<input type="button" value="▼"/>
--------	-------------	----------------------------------

**Figure 343: Action**

- Click Save.

## Custom IPS Signatures

This page displays the list of all the custom IPS patterns.

Custom IPS Patterns provide the flexibility to customize IPS for diverse network environments. Predefined IPS patterns included in the device cover common attacks while Custom IPS Patterns protect your network from uncommon attacks that are due to the use of proprietary server, custom protocol, or specialized applications used in the corporate network.



**Note:** Administrator can create Custom IPS Pattern and configure policies using them. However, the IPS scanning will be effective only if Network Protection module is subscribed.

## Add IPS Pattern

1. Go to **Protect > Intrusion Prevention > Custom IPS Signatures** and click **Add**.
2. Enter the IPS Signature details.

### Name

Enter a name to identify the Custom IPS Signature.

### Protocol

Select IPS protocol from the list.

**Available Options:** TCPUDPICMPALL

### Custom Rule

Specify IPS Signature definition.

Signature definition must begin with a keyword followed by the value enclosed between the double quotes and must end with semicolon (;)

Format: Keyword: "value";

For example, content: "USER JOHN";

If traffic with the content USER JOHN is detected, action defined in the policy will be taken.

Refer to Appendix B – IPS - Custom IPS Pattern Syntax for more details on creating IPS Pattern.

### Severity

Select the level of severity from the available options. Critical Major Moderate Minor Warning

### Recommended Action

Specify action to be taken on the selected policy when matching pattern is found.

#### Available Actions:

**Allow Packet** - Check each packet before taking action. **Drop Packet** - Drop packets. **Drop Session**

- Terminate entire session instead of scanning all the session packets to save resources and avoid getting high number of alerts. **Reset** - Send TCP reset packet to the originator. **Bypass Session** - Scan initial packets only. If the initial packets match the pattern then the rest of the session packets are not scanned and the traffic is allowed to pass.

In all the cases, device generates the log and alerts the Network Administrator.

Name *	<input type="text"/>
Protocol *	<input type="button" value="Select Here"/>
Custom Rule *	<input type="text"/>
Severity *	<input type="button" value="Select Here"/>
Recommended Action	<input type="button" value="Allow Packet"/>

**Figure 344: Add Custom IPS Signature**

3. Click Save.

## DoS & Spoof Prevention

The device provides several security options that cannot be defined by the security policies. This includes protection from several kinds of “Denial of Service attacks”. These attacks disable computers and circumvent security.

A Denial of Service (DoS) attack is a method that hackers use to prevent or deny legitimate users access to a service.

DoS attacks are typically executed by sending many request packets to a targeted server (usually Web, FTP, or Mail server), which floods the server’s resources, making the system unusable. Their goal is not to steal the information but disable or deprive a device or network so that users no longer have access to the network services/resources.

All servers can handle a traffic volume up to a maximum, beyond which they become disabled. Hence, attackers send a very high volume of redundant traffic to a system so it cannot examine and allow permitted network traffic. Best way to protect against the DoS attack is to identify and block such redundant traffic. Below are some DoS settings which can be used for identifying DoS attack:

### Packet rate per Source

Total number of connections or packets allowed to a particular user.

### Burst rate per Source

Maximum number of packets allowed to a particular user at a given time.

### Packet rate per Destination

Total number of connections or packets allowed from a particular user.

### Burst rate per Destination

Maximum of packets allowed from a particular user at a given time.

## How it works

When the burst rate is crossed, the device considers it as an attack. The device provides DoS attack protection by dropping all the excess packets from the particular source/destination. The device will continue to drop the packets till the attack subsides. Because the device applies threshold value per IP address, traffic from the particular source/destination will only be dropped while the rest of the network traffic will not be dropped at all.

Time taken to re-allow traffic from the blocked source/destination = time taken to subside the attack + 30 seconds

### For example:

Packet rate per source: 100 packets per second

Burst rate per source: 200 packets per second

When the user starts sending requests, initially he will be able to send 200 packets per second but once the 200 packets are received, in the next phase the user will only be able to send 100 packets per second. So in the next phase, if the user sends 150 packets per second, the device will consider it as an attack and drop 50 (150 -100) packets. The device will then only accept traffic from the user 30 seconds after having dropped the packets.

### **Threshold values**

The device uses packet rate and burst rate values as a threshold value to detect DoS attacks. These values depend on various factors like:

- Network bandwidth
- Nature of traffic
- Capacity of servers in the network

These values are applicable to the individual source or destination requests per user/IP address and not globally to the entire network traffic. For example, if the source rate is 2500 packets/minute and the network consists of 100 users then each user is allowed a packet rate of 2500 packets per minute

Configuring high values will degrade the performance and too low values will block the regular requests. Hence it is very important to configure appropriate values for both source and destination IP address.

### **Spoof Protection General Settings**

You can configure a MAC and/or IP address pair entry in the IP-MAC trusted list to improve the security of your network. Using MAC address filtering makes it more difficult for a hacker to guess and use a random MAC address or spoof a MAC address to gain access to your network as the traffic does not even reach your firewall.

Similarly, it is also possible to filter packets based on the IP-MAC pair. It prevents hosts which try to violate trusted IP-MAC. To make the restriction more granular, you can enable restriction on the zones.

#### **Enable Spoof Prevention**

If enabled, the device provides 3 ways to prevent spoofing using an IP-MAC trusted list:

- **IP Spoofing** – Packets will be dropped if a matching route entry is not available.
- **MAC Filter** – Packets will be dropped if the MAC addresses are not configured as trusted MAC.
- **IP-MAC Pair Filter** – Packets will be dropped if either IP or MAC address does not match with any entry in the IP-MAC trusted list. Packets will be allowed if both IP and MAC address are not defined as an entry in the IP-MAC trusted list.

#### **Restrict Unknown IP on Trusted MAC (Only applicable if Spoof Prevention is enabled)**

Enable the option, if you want to drop traffic from any IP address not in the trusted list for the trusted MAC address.

By default, it is disabled. When disabled, traffic from any IP address not in the trusted list will be allowed even if it is coming for the trusted MAC address.

Zone	LAN	WAN	DMZ	WiFi
<b>IP Spoofing</b>	Yes Enable at least for one zone.  The device will reverse lookup for the route of the source network and, if not available, packets will be dropped and logged.  Default: disabled for all zones	No	Yes	Yes

Zone	LAN	WAN	DMZ	WiFi
<b>MAC Filter</b>	<p>Yes</p> <p>It restricts the access of your network to the external hosts.</p> <p>As the device will drop all the requests from the MAC address not configured in the trusted list, please make sure to include MAC addresses of all your internal devices.</p> <p>If enabled, it is to be enabled for at least one zone.</p> <p>Default: disabled for all zones</p>	Yes	Yes	Yes

Zone	LAN	WAN	DMZ	WiFi
<b>IP-MAC Pair Filter</b>	Yes	No	Yes	Yes

The device will drop the request considering it as a spoofed request if:

- MAC address differs for the trusted IP address and
- IP address differs for the trusted MAC address

But, the request will be allowed if IP or MAC address does not exist at all in the list. Request is dropped if the IP-MAC

<input type="checkbox"/> Enable Spoof Prevention	<input type="checkbox"/> Restrict Unknown IP on Trusted MAC		
	IP Spoofing	MAC Filter	IP-MAC Pair Filter
LAN	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
WAN		<input type="checkbox"/>	
DMZ	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
WiFi	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

**Figure 345: Spoof Protection General Settings**

### Spoof Protection Trusted MAC

You can enable MAC address and/or IP address pair filtering to improve security. By enabling filtering, you define the devices that can access your network. It is also possible to import the trusted MAC list through a CSV (Comma Separated Value) file. When a user attempts to access the network, the device checks the MAC address and/or IP address from the list. User gets access to the network only if the MAC address and/or IP address are in the trusted MAC list, else the request is rejected.

The **Spoof Prevention Trusted MAC** section displays a list of all the MAC addresses configured as trusted MAC. The page also provides options to *add* a new MAC address, update the existing addresses, and *import* the list of addresses.

### DoS Settings

Attack definition can be defined both for source and destination.

#### SYN Flood

SYN Flood is the attack in which large numbers of connections are sent so that the backlog queue overflows. The connection is created when the victim host receives a connection request and allocates some memory resources to it. A SYN flood attack creates so many half-open connections that the system becomes overwhelmed and cannot handle incoming requests any more.

Configure packet rate (packets/minute) and burst rate (packets/second) for source and destination.

Select **Apply Flag** check box to apply the SYN flood definition and control the allowed number of packets.

**Source Traffic Dropped** displays number of source packets dropped in case source packet rate control is applied.

**Destination Traffic Dropped** displays the number of packets dropped in case destination packet rate control is applied.

Click on the link **Click Here** to view DoS attacks status. You will be redirected to **Protect > Intrusion Prevention > DoS Attacks**. Then click **SYN Flood** to view the real-time updates on flooding. It displays the source IP address - which was used for flooding and IP address which was targeted.

#### UDP Flood

User Datagram Protocol (UDP) Flood links two systems. It hooks up one system's UDP character-generating service, with another system's UDP echo service. Once the link is made, the two systems are tied up exchanging a flood of meaningless data.

Configure packet rate (packets/minute) and burst rate (packets/second) for source and destination.

Select **Apply Flag** check box to apply the UDP flood definition and control the allowed number of packets.

**Source Traffic Dropped** displays the number of source packets dropped in case source packet rate control is applied.

**Destination Traffic Dropped** displays the number of packets dropped in case destination packet rate control is applied

Click on the link **Click Here** to view DoS attacks status. It will redirect you to **Protect > Intrusion Prevention > DoS Attacks** and Click **UDP Flood** to view the real-time updates on flooding. It displays the source IP address - which was used for flooding and IP address which was targeted.

### TCP Flood

TCP attack sends huge amount of TCP packets so that the host/victim computer cannot handle, thereby denying service to legitimate TCP users.

Configure packet rate (packets/minute) and burst rate (packets/second) for source and destination.

Select **Apply Flag** check box to apply the TCP flood definition and control the allowed number of packets.

**Source Traffic Dropped** displays the number of source packets dropped in case source packet rate control is applied.

**Destination Traffic Dropped** displays the number of packets dropped in case destination packet rate control is applied

### ICMP/ICMPv6 Flood

ICMP/ICMPv6 attack sends huge amounts of packet/traffic so that the protocol implementation of the host/victim computer cannot handle, thereby preventing legitimate packets from getting through to their destination.

Configure packet rate (packets/minute) and burst rate (packets/second) for source and destination.

Select **Apply Flag** check box to apply the ICMP flood definition and control the allowed number of packets.

**Source Traffic Dropped** displays the number of source packets dropped in case source packet rate control is applied.

**Destination Traffic Dropped** displays the number of packets dropped in case destination packet rate control is applied

Click on the link **Click Here** to view DoS attacks status. It will redirect you to **Protect > Intrusion Prevention > DoS Attacks** and Click **ICMP/ICMPv6 Flood** to view the real-time updates on flooding. It displays the source IP address - which was used for flooding and IP address which was targeted.

### Dropped Source Routed Packets

Select **Apply Flag** check box to enable. This will block any source routed connections and prevent any packets with an internal address from entering your network.

### Disable ICMP/ICMPv6 Redirect Packet

An ICMP redirect packet is used by routers to inform the hosts what the correct route should be. If an attacker is able to forge ICMP redirect packets, he or she can alter the routing tables on the host and possibly weaken the security of the host by causing traffic to flow via another path.

Disable the option to prevent the attacker from forging ICMP redirect packets.

Default: enabled

### ARP Hardening

If enabled, the device will send an ARP reply only if the destination IP address is a local address configured on the incoming interface and both the sender and destination IP address are in the same subnet.

Attack Type	Source				Destination			
	Packet rate per Source (Packet/min)	Burst rate per Source (Packet/sec)	Apply Flag	Source Traffic Dropped	Packet rate per Destination (Packet/min)	Burst rate per Destination (Packet/sec)	Apply Flag	Destination Traffic Dropped
SYN Flood	12000	100	<input type="checkbox"/>	0	12000	100	<input type="checkbox"/>	0
UDP Flood	12000	100	<input type="checkbox"/>	0	18000	100	<input type="checkbox"/>	0
TCP Flood	12000	100	<input type="checkbox"/>	0	12000	100	<input type="checkbox"/>	0
ICMP/ICMPv6 Flood	120	100	<input type="checkbox"/>	0	300	100	<input type="checkbox"/>	0
Dropped Source Routed Packets	-	-	-	-	-	-	<input checked="" type="checkbox"/>	-
Disable ICMP/ICMPv6 Redirect Packet	-	-	-	-	-	-	<input checked="" type="checkbox"/>	-
ARP Hardening	-	-	-	-	-	-	<input type="checkbox"/>	-

[Click Here for DoS Attacks status](#)

[Apply](#)

**Figure 346: DoS Settings**

### DoS Bypass Rule

The device allows to bypass the DoS rule in case you are sure that the specified source will not be used for flooding or the device ignores flooding coming from the specified source. By default, VPN zone traffic is also subjected to DoS inspection. You can also bypass DoS inspection of the traffic coming from certain hosts of the VPN zone.

The **DoS Bypass Rule** section displays a list of all the bypass rule.

### Add Trusted MAC Address

1. Go to **Protect > Intrusion Prevention > DoS & Spoof Protection** and click **Add** under the **Spoof Protection Trusted MAC** section.
2. Enter trusted MAC address details.

#### MAC Address

Specify a MAC address to be added to the Trusted MAC list.

#### IPv4 Address

Specify an IPv4 address that is to be bound to the MAC address. Packets will be rejected if either MAC or IPv4 address does not match.

**Available Options:** **Static** – Specify an IP Address to be bound to the MAC address. Packets will be rejected if either MAC or IP address does not match. Multiple IP addresses separated by comma can be provided. **DHCP** – MAC address will be bound to the IP address leased by the device DHCP server as and when the IP is leased. Entry will be updated automatically when the leased IP address is updated.

To unbind the IPv4 address, select **None**.

#### IPv6 Address

Specify an IPv6 address that is to be bound to the MAC address. Packets will be rejected if either MAC or IPv6 address does not match.

**Available Options:** **Static** – Specify an IP Address to be bound to the MAC address. Packets will be rejected if either MAC or IP address does not match. Multiple IP addresses separated by comma can be provided. **DHCP** – MAC address will be bound to the IP address leased by the device DHCP server as and when the IP is leased. Entry will be updated automatically when the leased IP address is updated.

To unbind the IPv6 address, select **None**.

MAC Address \*

IPv4 Address

None  Static  DHCP

(Use comma to add multiple addresses)

IPv6 Address

None  Static  DHCP

(Use comma to add multiple addresses)

**Figure 347: Add Trusted MAC**

3. Click Save.

### Import Trusted MAC Addresses

Instead of adding the trusted entries individually, the device provides a facility to import the trusted list from a CSV (Comma Separated Value) file.

The format for the CSV file should be as follows:

1. First row of the CSV file has to be the header row: MAC Address,IP Association,IP Address.
2. The rest of the rows are values corresponding to the header fields .
3. Blank rows will be ignored.
4. An error message is displayed only for invalid rows.
5. Format of values:
  - Compulsory fields: MAC address and IP association.
  - Optional fields: IP address.
  - IP association must be **Static** or **DHCP/DHCPv6** or **None**.
  - For **Static** IP association, IP address must be available.
  - For **None/DHCP** type of IP association, IP address is not required.
  - For invalid MAC/IP address or IP association entry will be discarded.
  - Use comma to insert multiple static IP addresses.

1. Go to **Protect > Intrusion Prevention > DoS & Spoof Protection** and click **Import** under the **Spoof Protection Trusted MAC** section to import a CSV file.
2. Browse trusted MAC address file.

#### Trusted MAC Address File

To choose a CSV file, click the file selection button against **Trusted MAC Address File**.

3. Click **Upload File** to upload CSV file.

Trusted MAC Address File

No file selected.

**Figure 348: Import Trusted MAC Address CSV File**

### Create DoS Bypass Rule

1. Go to **Protect > Intrusion Prevention > DoS & Spoof Protection** and click **Add** under the **DoS Bypass Rule** section.
2. Enter bypass rule details.

#### IP Family

Select the IP family of the traffic to be bypassed.

#### Source IP/Netmask (*available only if selected IP Family is IPv4*)

Specify the source IP/Netmask.

Specify \* if you want to bypass entire network.

#### Destination IP/Netmask (*available only if selected IP Family is IPv4*)

Specify the destination IP/Netmask.

Specify \* if you want to bypass entire network.

#### Source IP/Prefix (*available only if selected IP Family is IPv6*)

Specify the source IP/prefix.

Specify \* if you want to bypass entire network.

#### Destination IP/Prefix (*available only if selected IP Family is IPv6*)

Specify the destination IP/prefix.

Specify \* if you want to bypass entire network.

#### Protocol

Select the protocol whose traffic is to be bypassed if generated from the specified source to destination.

**Available Options:** TCPUDPICMPAll Protocols

For example, if you select TCP protocol then DoS rules will not be applied on the TCP traffic from the specified source to destination.

#### Source Port

Specify port number for the source.

Specify \* if you want to bypass entire network.

#### Destination Port

Specify port number for the destination.

Specify \* if you want to bypass entire network.

IP Family	<input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6
Source IP/Netmask *	<input type="text"/>
Destination IP/Netmask *	<input type="text"/>
Protocol *	<input checked="" type="radio"/> TCP <input type="radio"/> UDP <input type="radio"/> ICMP <input type="radio"/> All Protocols
Source Port *	<input type="text"/>
Destination Port *	<input type="text"/>

**Figure 349: Add DoS Bypass Rule**

3. Click **Save**.

## Web

Use the web protection settings to identify and block the latest web threats. These settings let you control traffic and protect against threats and inappropriate web usage. Exceptions let you override settings as required for your business needs.

## Policies

With policies, you can control traffic using rules and advanced settings. The default set of policies describes some common restrictions.

To test and troubleshoot policies, click **Policy Test**.

Name	Description	In Use	Manage
Default Policy	A typical starter policy with options suitable for many organizations	<span style="color: orange;">⚠️</span>	<span style="color: orange;">+</span> <span style="color: orange;">(i)</span> <span style="color: orange;">Edit</span> <span style="color: orange;">Delete</span>
Block Upload	Block HTTP upload	<span style="color: orange;">⚠️</span>	<span style="color: orange;">+</span> <span style="color: orange;">(i)</span> <span style="color: orange;">Edit</span> <span style="color: orange;">Delete</span>
Default Workplace Policy	Deny access to categories most commonly unwanted in professional environments	<span style="color: orange;">⚠️</span>	<span style="color: orange;">+</span> <span style="color: orange;">(i)</span> <span style="color: orange;">Edit</span> <span style="color: orange;">Delete</span>

**Figure 350: Policies**

## Rules

Rules specify the following criteria:

- Users to whom the rule applies. These include groups and individual users.
- Activities that describe the type of usage to restrict. These include user activities, categories, URL groups, file types, and dynamic categories.
- Content filters to restrict web content that contains any terms in the lists specified.
- An action to take when the firewall encounters traffic that matches the rule criteria.

The firewall evaluates rules from highest to lowest. For example, a rule that allows all traffic that precedes a rule that restricts a specific type of traffic takes precedence and the subsequent rule is ignored.

**Name\***

**Description**

Add Rule

Users	Activities	Action	Constraints	Manage	Status
Anybody	HTTPUpload	<span style="color: red;">🚫</span>		<span style="color: orange;">+</span> <span style="color: orange;">(i)</span> <span style="color: orange;">Delete</span>	<span style="color: orange;">ON</span>
	Default Action	<span style="color: green;">✅</span>			

ⓘ Advanced Settings

**Figure 351: Rules**

## Migrating Policies from Previous Releases

This release supports up to 128 rules in a single policy. If you are migrating policies from a previous release that contain more than 128 rules, only the first 128 rules will be used.

Web policy rules now support combined activities. These include user activities, categories, URL groups, file types, and dynamic categories. To maintain the overall functionality of the policy, replace blocks of adjacent rules for different activities with a single rule that contains a group of activities. Please delete or consolidate rules as required.

### Add Policy

1. Go to **Protect > Web > Policies** and click **Add Policy**.
2. Type a name.
3. Click **Add Rule**.



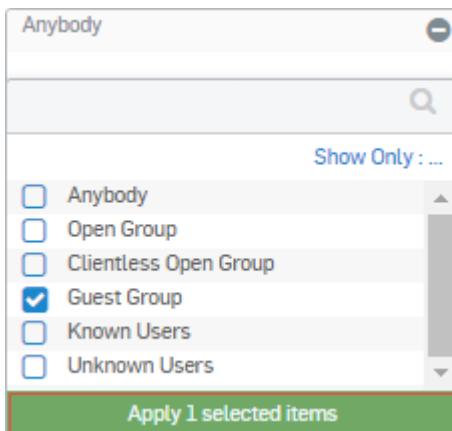
**Tip:** To use an existing rule as a template, click the Clone button ( ).

The firewall creates a default rule that blocks all web traffic for all users. The default rule is disabled.

Users	Activities	Action	Constraints	Manage	Status
= <input checked="" type="checkbox"/> Anybody	ALLWebTraffic				
Default Action					

**Figure 352: Add Rule**

4. Specify users.
    - a) In the new rule, move the pointer over the users field, click the user (“Anybody”), and then click **Add New Item**.
    - b) Clear the **Anybody** check box.
    - c) Select users.
- Tip:** You can filter the type of users to display by clicking **Show Only** and selecting a user type.
- d) Click **Apply selected items**.



**Figure 353: Select Users**

5. Specify activities and content filters.
  - a) Move the pointer over the activities field, click the activity (“AllWebTraffic”), and then click **Add New Item**.
  - b) In the **Activities** tab, clear the **All Web Traffic** check box.
  - c) Select activities.

**Tip:** You can filter the type of activities to display by clicking **Show Only** and selecting an activity type.

  - d) Click **Apply selected items**.
  - e) Click the **Content Filters** tab and enable the **and with content** check box.
  - f) Click **Add New Item** and select filters.
  - g) Click **Apply selected items**.
6. In the Action field, specify an action to take when the firewall encounters HTTP traffic that matches the selected criteria .

Select from the following options:

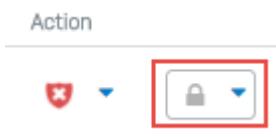
#### Options

Allow Warn Block Log

7. (Optional) Specify an action to take when the firewall encounters HTTPS traffic that matches the selected criteria.

**Note:** Follow these steps only if you want to specify an action for HTTPS traffic that is different from the one you specified for HTTP.

- a) Move the pointer to the right of the **Action** list.  
The firewall displays the **HTTPS Use Action** list.



**Figure 354: HTTPS Use Action**

- b) Select an option.

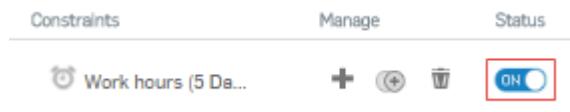
#### HTTPS Use Action

**Use Action:** Select this option to use the same action that is currently in effect for HTTP traffic. If you specify a different HTTP action at a later time, HTTPS action will also use that action. **Allow:** Always allow HTTPS traffic that matches the selected criteria. **Warn:** Always display a warning message when encountering HTTPS traffic that matches the selected criteria. **Block:** Always block HTTPS traffic that matches the selected criteria.

8. Move the pointer over the **Constraints** field and select a schedule.

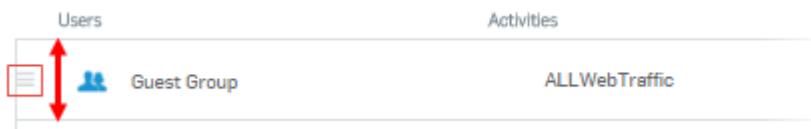
**Tip:** You can create a new schedule by clicking **Create new** and specifying criteria.

9. Click the On/Off switch to enable the rule.



**Figure 355: Enable Rule**

10. Click and drag the rule handle to position the rule in the hierarchy.



**Figure 356: Position Rule**

The firewall evaluates rules from highest to lowest. For example, a rule that allows all traffic that precedes a rule that restricts a specific type of traffic takes precedence and the subsequent rule is ignored.

11. Click **Advanced Settings** and specify settings for the policy.

#### Enable logging and reporting

Include this policy in logs and reports.

#### Prevent downloading of large files

Prevent downloading files greater than the size specified.

#### Restrict login domains for Google Apps

Restrict logging in to Google Apps only on the domains specified.

For your policies to take effect, add them to a firewall rule.

## User Activities

User activities combine web categories, file types, and URL groups in one container. For example, you can create a user activity to associate spyware and malware with a list of URLs. You can include user activities in web policies to control access to websites or files that match any of the specified criteria.

### Add User Activity

1. Go to **Protect > Web > User Activities** and click **Add**.
2. Type a name.
3. Click **Add New Item** and select categories.

Select from the following:

- Web categories
- File types
- URL groups

**Note:** Categories are evaluated using ‘OR’. Only one category must return true in order to match traffic.

**Tip:** You can filter the type of categories to display by clicking **Show: All** and selecting a category type.

The screenshot shows a 'Add User Activity' dialog box. In the 'Name' field, 'Suspected spyware' is entered. In the 'Category' section, a list titled 'Spyware & Malware' is shown. One item, 'Phishing sites', is selected with a checkmark. A green button at the bottom right says 'Apply 1 selected items'.

**Figure 357: Add User Activity**

## Categories

With web categories, you can organize and classify domains in a container. The default categories define some common content types. You can use categories within policies to restrict access to websites.

### Add Category

1. Go to **Protect > Web > Categories** and click **Add**.
2. Type a name.
3. Specify details.

### Classification

Use classifications to group content types. Select from the following options:

- **Productive**
- **Unproductive**
- **Acceptable**
- **Objectionable**

### Traffic Shaping Policy

If you want to apply a bandwidth restriction, choose a traffic shaping policy.

### Configure Category

Specify domains and keywords for the category using a configuration type. Select from the following options:

- **Local** - Define domains and keywords that are specific to your organization. To import a domain or keyword list, click **Choose File** and select a text file. To create a domain or keyword list, type a domain or keyword in the **Search/Add** text box and click the Add button (+).
- **External URL Database** - An external URL database contains a list of domains that is maintained by a third party. These include, for example, country-specific blacklists and open-source URL categorization lists. To specify an external URL database, type a URL in the **Search/Add** text box and click +. The firewall checks for updates every two hours.

Acceptable formats: .tar, .gz, .bz, .bz2, and .txt

Name \*

Description

Classification \*

Traffic Shaping Policy

Configure Category \*

Import Domain/Keyword

Domain/Keyword \*

Domain Keyword

Search / Add +

Search / Add +

**Figure 358: Add Category****4. Specify Advanced Settings.****Override Default Denied Message**

Select this option to define a custom message that will be shown to the user when a website is blocked as a result of this category.

Blocked Message

Override Default Blocked Message

```
<b><BR><font class=accessdeniedtextfont >This is a message from the IT Department.</font><BR><BR>The web site you are trying to access: <BR><font class=accessdeniedcategoryfont >[url]</font><BR><font class=accessdeniedtextfont >is listed as a site within the category </font><font class=accessdeniedcategoryfont>[category]</font><BR><BR><font class=accessdeniedtextfont > Current Internet Access Configuration for you does not allow visiting sites within this category at this time.<BR><BR>If the website has been erroneously blocked, please <a href="#" class=accessdeniedcategoryfont> onclick="callReevaluationFunction()"</a> submit</a> it for re-evaluation.</font></b>
```

HTML Input

**Figure 359: Advanced Settings****Related concepts**

[Firewall](#) on page 303

Firewall rules are security rule-sets to implement control over users, applications or network objects in an organization. Using the firewall rule, you can create blanket or specialized traffic transit rules based on the requirement. This page provides centralized management for the entire set of device firewall rules. Sophos XG Firewall implements a single pane of management to secure all enterprise applications using configuration templates for various rule types.

[Traffic Shaping](#) on page 297

**URL Groups**

URL groups contain one or more URLs that you can use in web policies to block or allow access to websites.

**Add URL Group**

1. Go to **Protect > Web > URL Groups** and click **Add**.
2. Type a name.

3.

Type a URL in the **Search/Add** text box and click the Add button (  ).



The screenshot shows a configuration interface for adding a URL group. It includes fields for 'URL Group Name \*' (with a required asterisk), 'Description', and 'Domain Names to match \*' (also with a required asterisk). A note to the right states: 'The URL Group will match any requests for these domains or their subdomains.' At the bottom are 'Search / Add' and 'Add' buttons.

**Figure 360: Add URL Group**

## Exceptions

With exceptions, you can override protection settings for web traffic that matches the specified criteria. For example, you can create an exception to skip HTTPS decryption for sites that contain confidential data. The default set of exceptions specifies some common override behaviors.

Override behaviors now include Sandstorm.

 **Note:** Existing exceptions that skip malware scanning now also skip Sandstorm analysis.

### Add Exception

1. Go to **Protect > Web > Exceptions** and click **Add Exception**.
2. Type a name.
3. Specify web traffic criteria.

 **Note:** The firewall evaluates all types of criteria specified using the “AND” operator. For example, if you specify URL patterns and website categories, both types must return true in order to match traffic. However, within each category, criteria are evaluated using “OR”.

#### URL pattern matches

Match web traffic according to the specified URL or pattern, for example, example.com. Regular expressions are allowed here. For example, ^([A-Za-z0-9.-]\*\.)?example\.com/ matches all subdomains of example.com.

 **Note:** You must specify pattern matches using ASCII characters. For information about converting non-ASCII characters, refer to [RFC 3490, Internationalizing Domain Names in Applications](#).

#### Website categories

Match web traffic according to the specified web categories.

#### Source IP addresses

Match web traffic that originates from the specified IP addresses.

#### Destination IP addresses

Match web traffic going to the specified IP addresses.

**Web Protection Exception**

Name \*

Description

For web traffic matching these criteria:

- URL pattern matches
  - Search / Add
  - + (Add)
- Web site categories
  - Add New Item
- Source IP addresses [end-user's address]
  - Search / Add
  - + (Add)
- Destination IP addresses [web site address]

Skip the selected checks or actions:

- HTTPS Decryption
- Malware and Content Scanning
- Sandstorm
- Policy Checks

**Figure 361: Add Exception**

- Specify an action to skip when the firewall encounters traffic that matches the criteria.

#### HTTPS Decryption

Do not decrypt HTTPS for traffic that meets the specified criteria.



**Note:** If you disable HTTPS decryption, the firewall will not perform any other check that relies on decrypted traffic, such as malware scanning. However, the firewall will continue to scan HTTP traffic that matches the exception.

#### Malware and Content Scanning

Do not scan traffic that meets the specified criteria for malware or content as specified in a content filter.

#### Sandstorm

Do not send files that are downloaded using the specified criteria to Sandstorm for analysis.

#### Policy Checks

Do not check policies for traffic that meets the specified criteria.

## File Types

A file type is a classification that is determined by file extension and MIME header. You can include file types in web policies to control access to files that match the specified criteria. The default file types contain some common criteria and you can create additional types.

### Using File Types with Policy Rules

You can create file types to control access to files on a more granular level. For example, you may want to allow access to SQL files but deny access to all other database files. In this case, you would create a file type for SQL files and a policy that specifies the following rules in the following order:

1. Allow access to SQL files
2. Block access to all database files

### Add File Type

1. Go to **Protect > Web > File Type** and click **Add**.

2. Type a name.

3. (Optional) Select a template.

You can select from predefined or custom file types. If you do not wish to use a template, choose **Blank**.

4. Specify the file extension and MIME header.

The screenshot shows a form for adding a file type. The fields are as follows:

- Name \***: A text input field labeled "Name".
- Description**: A text input field labeled "Description".
- Template**: A dropdown menu set to "Blank".
- File Extension \***: A text area labeled "Add Extensions here".
- MIME Header \***: A text area labeled "Add MIME Headers here".

Both the "File Extension" and "MIME Header" sections include a note at the bottom right: "Use comma as a separator to enter multiple entries."

**Figure 362: Add File Type**

### Surfing Quotas

Surfing quota policy allows you to assign the duration of Internet surfing time to users and groups.

- Duration of Internet access can be cyclic or non-cyclic.
- You can apply the surfing quota policy to users.

The device is shipped with the following predefined policies. Predefined policies can be applied straight away to users and groups.

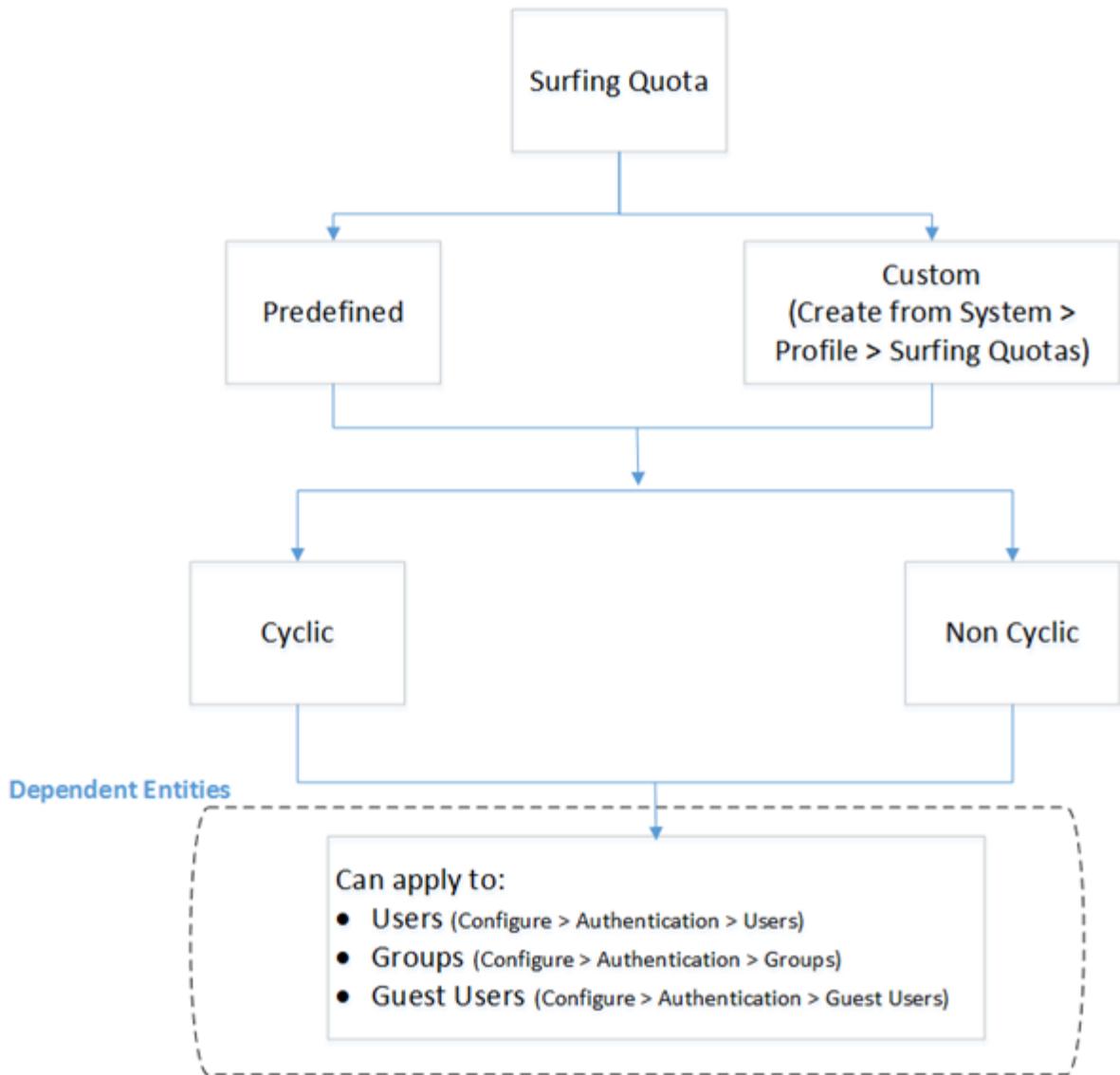
- Unlimited Internet Access
- 1 Month Unlimited Access
- 1 Month 100 hours
- Monthly 100 hours Cyclic
- Daily 1 hour Cyclic
- Weekly 7 hours Cyclic



**Note:**

1. Users generally belong to a group. If the surfing quota policy applied to the user differs from the one applied to the user's group, the user's policy takes priority.
2. For details of policies and rules to which the surfing quota policy can be applied, view the following diagram.

### Surfing Quota Policy: Basic Flow



### Add Surfing Quota

To assign the duration of Internet surfing time to users and groups, you can create surfing quota policies. These policies are then applied to users (**Configure > Authentication > Users**) and groups (**Configure > Authentication > Groups**).

The **Add Surfing Quota Policy** page allows you to create a surfing quota policy.

1. Go to **Protect > Web > Surfing Quotas** or **System > Profiles > Surfing Quotas** and click **Add** on the upper right side.

**Note:** Surfing Quota policies can also be created when applying the policy to users or groups from the respective pages. The Surfing Quota page displays the full list of predefined and custom policies.

2. Enter the details.

**Name**

Enter a unique name to identify the policy.

**Description**

Enter a description for the surfing quota policy.

**Cycle Type**

Select the cycle type.

**Available Options:** **Cyclic:** Duration of Internet access recurs for each cycle. **Non-Cyclic:** When the specified time limit ends, the user is disconnected.

**Cycle Hours (*available only if Cycle Type is Cyclic*)**

Specify the cycle hours in hours and minutes. Select the cycle from the drop-down list. Cycle hours define the upper limit of surfing hours for daily, weekly, monthly or yearly cycles.

At the end of each cycle, cycle hours are reset to zero.

Example: If cycle hours specified are 7 hours 30 minutes for a daily cycle, they are reset to zero at the end of each day whether cycle hours are fully or partially used or remain unused.

**Validity**

Select **Unlimited** if you do not want to restrict the validity period. Clear the check box to specify the validity period of Internet access.

**Maximum Hours**

Select **Unlimited** if you do not want to restrict the maximum allowed surfing duration. Clear the check box to specify the maximum duration (in hours and minutes) of surfing time allowed across the validity period.

Example: Cyclic Policy

Cycle Hours: 5 hours per day

Validity: 5 days

Maximum Hours: 20 hours

If the user accesses Internet for 5 hours each day, the user will have used 20 hours of Internet access by the end of the fourth day and hence will be disconnected.

Example: Non-Cyclic Policy

Validity: 10 days

Maximum Hours: 10 hours

The user is disconnected at the end of 10 hours even if the validity period does not expire.

The screenshot shows a configuration interface for a surfing quota policy. The fields include:

- Name \***: Enter Surfing Quota Policy
- Description**: Enter Description
- Cycle Type**: Cyclic (radio button selected)
- Cycle Hours \***: 00 Hour(s) & 00 Minute(s) per Day
- Validity \***: Unlimited Day(s)
- Maximum Hours \***: Unlimited Hour(s) & 00 Minutes

**Figure 363: Add Surfing Quota Policy**

3. Click Save.

## User Notifications

The firewall displays notifications to users when a web policy is set to block access or warn before connecting. Use these settings to create and preview notifications.

To specify an image to display on notification pages, enable the **Use custom images** check box and choose images.

To create a block notification, enable the **Use custom block message** check box and type a message.

To create a warning notification, enable the **Use custom warn message** check box and type a message.

You can preview current messages by clicking the preview links.

## Applications

---

This section provides facilities to control and manage the applications shipped with the device.

The following pages are accessible:

- [Application List](#) on page 401: Displays all applications available for use.
- [Application Filter](#) on page 402: Enables you to control access to the applications.
- [Traffic Shaping Default](#): Apply traffic shaping policy to the application category or to the individual application within the category.

## Application List

This page displays all the applications available for use.

The device can identify and control applications that use standard ports, non-standard ports, or port hopping, or that tunnel through encrypted SSL traffic. This feature enables prioritization of applications based on user identity, time, and bandwidth, allowing great flexibility, visibility, and control. The device also provides implementation of application-based bandwidth management, accelerating critical applications while blocking malware-laden sites through web filtering. Organizations can group applications as per their requirements into business-critical, entertainment, communication, or collaboration, and can control access through security policies.

 **Note:** You need a subscription to Web Protection before you can use this feature. Check its features by taking a free trial. (See **System > Administration > Licensing**)

The device is shipped with a set of predefined applications. These applications are classified based on their risk level, characteristics and technology, offering more granular controls.

The total number of application signatures included depends on the Application Signatures Database used by the device.

The application list can be filtered based on name of the application, category of the application, risk, characteristics, and technology.

## Application Filter

This page displays a list of all the predefined and custom policies.

An Application Filter Policy controls a user's application access. It specifies which user has access to which applications and allows you to define powerful security policies based on almost limitless policy parameters like:

- Individual users
- Groups of users
- Time of day

The device is shipped with the following predefined policies for application filters to address common use cases:

- **Allow All:** By default, allows access to all the categories except the specified categories. Access to the specified categories depends on the strategy defined for each category.
- **Deny All:** By default, denies access to all the categories except the specified categories. Access to the specified categories depends on the strategy defined for each category.
- **Block filter avoidance apps:** Drops traffic from applications that tunnel other applications, proxy and tunnel applications, and from applications that can bypass firewall policy. These applications allow users to anonymously browse the Internet by connecting to servers on the Internet via encrypted SSL tunnels. This, in turn, enables users to bypass network security measures.
- **Block generally unwanted apps:** Drops generally unwanted application traffic. This includes applications such as file transfer, proxy & tunnel, risk prone, peer to peer networking (P2P) and applications that cause loss of productivity.
- **Block high risk (Risk Level 4 and 5) apps:** Drops traffic from applications that are classified under 'high risk' applications (Risk Level- 4 and 5).
- **Block peer to peer (P2P) networking apps:** Drops traffic from applications that are categorized as P2P applications. P2P could be a mechanism for distributing Bots, Spywares, Adware, Trojans, Rootkits, Worms and other types of malwares. It is generally advised to have P2P applications blocked in your network.
- **Block very high risk (Risk Level 5) apps:** Drops traffic from applications that are classified under 'very high risk' applications (Risk Level- 5).

These predefined policies are immediately available for use. You can also define custom policies to specify different levels of access for different users to meet your organization's requirements.

The page also provides options to add a new policy, update the parameters of an existing policy, delete a policy, add a filtering rule to a policy, or delete a filtering rule attached to a policy.



**Note:** You cannot edit/delete **Allow All** and **Deny All** predefined policies.

In application filter policies, web proxy detects applications that use HTTPS.

### Add Application Filter Policy

This page lets you configure custom policies to define different levels of access for different users to meet your organization's requirements.

1. Go to **Protect > Applications > Application Filter** and click **Add**.
2. Enter the Application Filter Policy details.

#### Name

Enter a name to identify the Application Filter Policy.

#### Description

Enter description for the Application Filter Policy.

#### Template

Select template for the Application Filter Policy.

The screenshot shows a form for creating an Application Filter Policy. It includes fields for 'Name \*' (with a required asterisk), 'Description', and 'Template' (set to 'Allow All').

Name *	<input type="text"/>
Description	<input type="text"/>
Template	Allow All

**Figure 364: Application Filter**

3. Click Save.
4. Once the policy is added, next step is to add a rule for configuring filtering criteria.

**Note:** Rules can be added for custom policies only.

#### Add Application Filter Policy Rules

Use the **Add Application Filter Policy Rules** page to configure a new rule for Application Filter Policy.

The **Add Application Filter Policy Rules** page allows you to manually configure a new rule.

1. Go to **Protect > Applications > Application Filter** and click .
2. Click **Add** under Application Filter Policy.
3. Enter the application filter details.

#### Category

Select Application Category from the list of available categories.

#### Risk

Select the level of risk from the available options. Select All1 - VERY LOW 2 - LOW3 - MEDIUM 4 - HIGH5 - VERY HIGH

#### Characteristics

Select the characteristics from the available options. Select AllExcessive BandwidthProne to misuseTransfer filesTunnels other appsVulnerabilities Widely usedLoss of productivityCan bypass firewall policy

#### Technology

Select the technology from the available options. Select AllBrowser BasedClient ServerNetwork ProtocolP2P

#### Smart Filter (available only if Select All is selected)

Enter the partial or full name of the application category to be filtered.

The screenshot shows a search interface with dropdown menus for 'Category', 'Risk', 'Characteristics', 'Technology', and a 'Smart Filter' input field. The 'Smart Filter' field contains the text 'Proxy and Tunnel'.

**Figure 365: Application Filter Criteria**

4. Enter the list of matching applications.

#### Select All

Click to select all the Applications from the list.

Applications are available based on the Application Filter Criteria.

**Select Individual Application**

Click to select the Applications from the list.

Applications are available based on the Application Filter Criteria.

**Search**

Specify the name of the application in the textbox to be searched.

This option is available, only if option “Select Individual Application” is selected.

**Name**

Displays name of the Applications under the Category selected. You can also select more than one application using the checkbox.

**Description**

Displays description of the Application.

**Category**

Displays category of the Application.

**Risk**

Displays the risk factor involved with the Application.

**Characteristics**

Displays the characteristics of the Application.

**Technology**

Displays the technology utilized for the Application.

<input type="checkbox"/> Select All	<input type="radio"/> Select Individual Application	Name	Description	Category	Risk	Characteristics	Technology
<input checked="" type="checkbox"/>		4everproxy Proxy	4everproxy Proxy	Proxy and Tunnel	3 - Medium	Can bypass firewall ...	Browser Based
<input checked="" type="checkbox"/>		AOL Desktop	AOL Desktop	Proxy and Tunnel	3 - Medium	Tunnels other apps,T...	Client Server
<input checked="" type="checkbox"/>		Air Proxy	Air Proxy	Proxy and Tunnel	3 - Medium	Prone to misuse,Can ...	Browser Based
<input checked="" type="checkbox"/>		Amaze VPN	Amaze VPN	Proxy and Tunnel	5 - Very High	Loss of productivity...	Client Server
<input checked="" type="checkbox"/>		Aniscartujo Web Proxy	Aniscartujo Web Proxy	Proxy and Tunnel	3 - Medium	Can bypass firewall ...	Browser Based
<input checked="" type="checkbox"/>		Anonymox	Anonymox	Proxy and Tunnel	4 - High	Can bypass firewall ...	Client Server

List of Matching Applications (1 - 50 of 256) \* Scroll down to view more signatures

**Figure 366: List of Matching Applications**

5. Enter the action you want to perform.

**Action**

Select an Action for the Policy from the available options. Allow Deny

**Schedule**

Select schedule from the list available in the dropdown list.

Action *	<input checked="" type="radio"/> Allow <input type="radio"/> Deny
Schedule *	All the Time

**Figure 367:**

6. Click Save.

## Traffic Shaping Default

The Traffic Shaping Default page allows you to view the list of all application categories. This page also provides the option to edit the category or application to apply a traffic shaping policy.

The applications shipped with the device are grouped into categories. These categories can be used in filtering policy and bandwidth restriction can be applied to the category or to the individual application within the category.

The categories list can be filtered based on name of the category. Use the or toggle beside the category name to expand and collapse the list of applications grouped in the respective category.

### Configure Traffic Shaping Policy for Category or Application

Use this page to configure traffic shaping policy.

This page allows you to configure traffic shaping policy for category or application.

1. Go to **Protect > Applications > Traffic Shaping Default** and click .
2. Enter the details.

#### Name

Displays the name of the Application Filter Category or Application.

#### Traffic Shaping Policy

Select a policy or click **Create new** to create a new traffic shaping policy for the application/application category.

Traffic Shaping policy allocates and limits the bandwidth usage of the user, web category, application category.

3. Click **Save**.

---

## Wireless

Wireless Protection allows you to configure the following:

- *Wireless Networks*: Create and manage Wireless Networks.
- *Mesh Networks*: Create and manage Mesh Networks.
- *Access Points*: Provides an overview of the access points known to the device.
- *Access Point Groups*: Allows you to organize access points in groups.
- *Hotspots*: Add/remove Hotspots and apply filtering policies.
- *Hotspot Voucher Definition*: Manage different voucher definitions for Hotspot access vouchers.
- *Rogue AP Scan*: Schedule scanning to discover authorized APs and rogue APs.

## Wireless Client List

The **Wireless Client List** page displays a live snapshot of currently managed APs, broadcasted SSIDs (wireless networks), wireless clients connected through SSID to AP and mesh networks.

### Show by SSID/Show by AP

The administrator can filter currently connected clients by **Access Point** or **SSID**

The page provides a list of wireless clients along with their name, IP address, MAC address, signal, last data transfer rate, connection time, frequency, vendor.

Name	IP Address	MAC Address	Signal	Last-TX Rate	Connection Time	Frequency	Vendor
SSID: admin							

**Figure 368: Wireless Client List**

## Wireless Networks

The **Wireless Networks** menu allows managing the wireless networks connected to the device.

 **Note:** You can also view the wireless network status on the **Protect > Wireless > Wireless Client List**

The page provides a list of all configured wireless networks along with their name, SSID, status, client traffic mode, encryption mode used and frequency band.

<input type="checkbox"/>	Name	SSID	Status	Client traffic	Encryption Mode	Frequency Band	Manage
<input type="checkbox"/>	GuestAP	GuestAccess		Separate Zone	No Encryption	2.4 and 5 GHz	 
<input type="checkbox"/>	Sophos	Sophos		Bridge to AP LAN	WPA2 Personal	2.4 GHz	 

**Figure 369: Wireless Networks List**

### Add a New Wireless Network

This page describes how to add a new wireless network.

Newly created wireless networks can be used in definitions for access points and access point groups.

1. Go to **Protect > Wireless > Wireless Networks** and click the **Add** button.
2. Specify the **General Settings** settings.

#### Name

Specify a descriptive name for the network.

#### Description

Enter a description for the wireless network that helps you to identify it.

#### SSID

Enter the Service Set Identifier (SSID) for the network which will be seen by clients and allow them to identify the wireless network. The SSID may consist of 1-32 *ASCII printable characters*.

#### Security Mode

Select a security mode from the drop-down list.

Default: WPA 2 Personal.

 **Note:** We recommend to use WPA2. For security reasons, we recommend not to use WEP unless there are clients using your wireless network that do not support one of the other methods.

When using an enterprise authentication method, you also need to configure a RADIUS server on the **Configure > Authentication > Servers** page. As NAS ID of the RADIUS server enter the wireless network name.

 **Note:** Sophos XG Firewall supports the IEEE 802.11r standard in WPA2 (PSK/Enterprise) networks to reduce roaming times. Clients also need to support the IEEE 802.11r standard.

**Passphrase/PSK (available only if WPA Personal, WPA2Personal, or WPA2/WPA Personal security mode is selected)**

Specify the passphrase to protect the wireless network from unauthorized access and repeat it in the **Confirm Passphrase/PSK** field. The passphrase may consist of 8-63 ASCII printable characters.

**Key (*available only if WEP Open security mode is selected*)**

Specify a WEP key that consists of exactly 26 hexadecimal characters.

### Client Traffic

From the dropdown list select how the wireless network is to be integrated into your local network.

Available options:

- Separate Zone
- Bridge to AP LAN
- Bridge to VLAN

Default: **Separate Zone**.

#### Separate Zone

The wireless network is handled as a separate network, having an IP address range of its own. Using this option, after adding the wireless network, proceed as described in the chapter [Next Steps for Separate Zone Networks](#).



**Note:** When switching an existing **Separate Zone** network to **Bridge to AP LAN** or **Bridge to VLAN**, a previously configured WLAN interface will be deleted.

#### Zone

From the dropdown list select a zone where the wireless network should be broadcast.

Default: **WiFi**.

#### IP Address

Assign an IP address to the wireless network.

#### Netmask

Select a subnet mask for the IP address.

#### Bridge to AP LAN

You can bridge a wireless network into the network of an access point, which means that wireless clients share the same IP address range. Using this option, after adding the wireless network, proceed as described in the chapter [Next Steps for Bridge to AP LAN Networks](#).

#### Bridge to VLAN (*not available for local WiFi devices*)

You can decide to have this wireless network's traffic bridged to a VLAN of your choice. This is useful when you want access points to be in a common network separate from the wireless clients.

#### Bridge to VLAN ID

Specify the VLAN ID of the network that the wireless clients should be part of.

#### Client VLAN ID (*only available with an enterprise security mode*)

Select how the VLAN ID is defined.

- **Static:** Uses the VLAN ID defined in the **Bridge to VLAN ID** field.
- **RADIUS & Static:** Uses the VLAN ID delivered by your RADIUS server: When a user connects to one of your wireless networks and authenticates at your RADIUS server, the RADIUS server tells the access point what VLAN ID to use for that user. Thus, when using multiple wireless networks, you can define per user who has access to which internal networks. If a user does not have a VLAN ID attribute assigned, the VLAN ID defined in the **Bridge to VLAN ID** is used.

Name *	<input type="text" value="wlnet2"/>
Description	<input type="text"/>
SSID *	<input type="text"/>
<hr/>	
Security Mode	<input type="text" value="WPA2 Personal"/>
Passphrase/PSK *	<input type="text" value="Passphrase/PSK"/> <input type="text" value="Confirm Passphrase/PSK"/>
Client traffic *	<input type="text" value="Separate Zone"/>
Zone	<input type="text" value="WiFi"/>
IP Address *	<input type="text"/>
Netmask *	<input type="text" value="/24 (255.255.255.0)"/>

**Figure 370: Add Wireless Network**

### 3. Specify the Advanced Settings.

**Encryption (available only if the WPA, WPA2, or WPA2/WPA encryption mode is selected)**

Select an encryption algorithm, which can be **AES**, **TKIP** or **TKIP&AES**.



**Note:** For security reasons and better performance, we recommend you to use AES.

### Frequency Band

Access points assigned to this wireless network will transmit on the selected frequency band(s). The 5 GHz band generally has a higher performance, lower latency, and is typically less disturbed. Hence it should be preferred for e.g. VoIP communication.

### Time-based Access

Select this checkbox to enable the wireless network access according to a time schedule.

**Select Active Time (available only if Time-based Access is selected)**

Select a schedule definition which determines when the wireless network is enabled. You can add a new schedule definition by clicking **Add New Item**.

### Client Isolation

Clients within a network usually can communicate with one another. If you want to prevent this, for example in a guest network, select **Enabled** from the drop-down list.

### Hide SSID

If you want to hide the wireless network's SSID, select the **Enable** checkbox. Please note that this is not a security feature.

**Fast Transition (available only if WPA2 Personal/Enterprise security mode is selected)**

Wireless networks with WPA2 security use the IEEE 802.11r standard. If you want to prevent this, select **Disabled** from the drop-down list.

### MAC Filtering

To restrict the MAC addresses allowed to connect to this wireless network, select **Blacklist** or **Whitelist**. With **Blacklist**, all MAC addresses are allowed except those listed on the **MAC List**. With **Whitelist**, all MAC addresses are prohibited except those listed on the **MAC List**.

MAC hosts added under **System > Hosts and Services > MAC Host** will be displayed in the **MAC List**.

<b>Advanced Settings</b>	
Encryption	TKIP (only abg)
Frequency Band	2.4 and 5 GHz
Time-based Access	<input checked="" type="checkbox"/> Enable
Client Isolation	Disabled
Hide SSID	<input checked="" type="checkbox"/> Enable
Fast Transition	Disabled
MAC Filtering	<input checked="" type="radio"/> None <input type="radio"/> Whitelist <input type="radio"/> Blacklist

**Figure 371: Wireless Network Advanced Settings**

- Click **Save**.

### Next Steps for Separate Zone Networks

This page describes how to configure a separate zone network.

When you add a wireless network with the option **Separate Zone**, a new corresponding virtual hardware interface will be added automatically, e.g., wlnet1. To be able to use the wireless network, some further manual configuration steps are required.

- Enable DHCP for the wireless clients.

For your clients to be able to connect to Sophos XG Firewall, they need to be assigned an IP address and a default gateway. Therefore, on the **Protect > Network > DHCP** page, set up a DHCP server for the interface.

- Create a network policy on the **Policies** page to provide Internet access to the wireless clients.

You can now assign the wireless network to the AP at **Protect > Wireless > Access Points**.

### Bridge to AP LAN Networks with Local Devices

For Local Wi-Fi Devices you need to configure some extra settings to enable bridging for the AP LAN.

- Edit the Local Wi-Fi Device on the **Protect > Wireless > Access Points** page and select the wireless network.
- Either create a new bridge interface on the **Protect > Network > Interfaces** page to use the wireless interface in bridge mode or edit the interface on the **Configure > Network > Interfaces** page, select a zone and provide an IP address to use the interface in gateway mode.
- If you want to use the interface in gateway mode, create a DHCP server on the **Protect > Network > DHCP** page so that the client can receive an IP.

Wireless clients can now connect to the wireless network.

## Access Point Overview

This page provides an overview of the access points (AP) known to the system.

## Access Point Types

Sophos XG Firewall currently provides the following types of dedicated access points:

**Table 3:**

Name	Standards	Band	FCC regulatory domain (mainly US)	ETSI regulatory domain (mainly Europe)
AP 10	802.11b/g/n	2.4 GHz		
AP 15	802.11b/g/n	2.4 GHz	Channels 1-11	Channels 1-13
AP 15c	802.11b/g/n	2.4/5 GHz dual-band/ single-radio	Channels 1-11	Channels 1-13
AP 30	802.11b/g/n	2.4 GHz		
AP 50	802.11a/b/g/n	2.4/5 GHz dual-band/ dual-radio	Channels 1-11, 36-48, 149-165	Channels 1-13, 36-48
AP 55	802.11a/b/g/n	2.4/5 GHz dual-band/ dual-radio	Channels 1-11, 36-48, 149-165	Channels 1-13, 36-64, 100-116, 132-140
AP 55C	802.11a/b/g/n	2.4/5 GHz dual-band/ dual-radio	Channels 1-11, 36-48, 149-165	Channels 1-13, 36-64, 100-116, 132-140
AP 100	802.11a/b/g/n/ac	2.4/5 GHz dual-band/ dual-radio	Channels 1-11, 36-48, 149-165	Channels 1-13, 36-64, 100-116, 132-140
AP 100C	802.11a/b/g/n/ac	2.4/5 GHz dual-band/ dual-radio	Channels 1-11, 36-48, 149-165	Channels 1-13, 36-64, 100-116, 132-140

Sophos XG Firewall also provides the following dedicated outdoor access points:

**Table 4:**

Name	Standards	Band	FCC regulatory domain (mainly US)	ETSI regulatory domain (mainly Europe)
AP 100X	802.11a/b/g/n/ac	2.4/5 GHz dual-band/ dual-radio	Channels 1-11, 36-64, 100-116, 132-140	Channels 1-13, 100-116, 132-140

Sophos XG Firewall also provides the following Wi-Fi Remote Ethernet Devices:

**Table 5:**

Name	Standards	Band
RED 15w	802.11a/b/g/n	2.4/5 GHz dual-band

Sophos XG Firewall also provides the following local Wi-Fi devices:

**Table 6:**

Name	Standards	Band
SG 105w/115w	802.11a/b/g/n	2.4/5 GHz dual-band
SG 125w/135w	802.11a/b/g/n/ac	2.4/5 GHz dual-band

 **Note:** Because of the bandwidth on the APs with ac standard there may be an automatic channel change in some cases. For example, if you select channel 36 the AP could choose channel 40 instead because it provides a better connection. The channel shown on the **Access Points** page represents the primary channel. This can affect all AP 100 appliances (AP 100, AP 100C and AP 100X) and all SG appliances with integrated access (SG 105w/115w and SG 125w/135w).

 **Note:** \*This article includes information on EOL hardware, which may continue to work but will be unsupported.

### Access Points

The **Access Points** menu allows you to manage the access points (AP) known to the system.

Sophos XG Firewall distinguishes between active, inactive and pending APs. To make sure that only genuine APs connect to your network, APs need to be authorized first.

Access points can be temporarily disabled. When an AP is physically removed from your network, you can delete from the table by clicking the **Delete** button. As long as the AP remains connected to your network, it will automatically re-appear in the **Pending Access Points** list after deletion. Sophos XG Firewall appliances with on-board Wi-Fi cannot be deleted from the AP list.

#### Protect > Wireless > Access Points

This page displays a list of all the active/inactive access points as well as a list of all the pending access points. It provides options to edit or delete access points and to accept pending access points. You can also view access points on the **Protect > Wireless > Wireless Client List** page.

#### Active/Inactive Access Points

For each access point, the list shows you:

##### ID

Access point ID

##### Label

Label of the AP, which allows it to be identified easily in the network.

##### Status

Status of the access point (active/inactive). Active APs are connected, configured, and running. Inactive APs have been configured in the past but are currently not connected to Sophos XG Firewall. If an AP remains in this state for more than five minutes, please check the network connectivity of the AP and the configuration of your system.

##### Channel

Channel the AP transmits on.

##### Group

Access point group the AP is assigned to.

##### Country

Country where the AP is located.

##### MAC

MAC address of the AP.

##### IP/Last Seen

IP address of an active AP or the last seen IP address of an inactive AP.

#### Type

Type of the AP

<input type="checkbox"/>	ID	Label	Status	Channel	Group	Country	MAC	IP/Last Seen	Type	Manage	Delete
No Records Found											

**Figure 372: Active/Inactive Access Points**

#### Pending Access Points

Here, APs are listed that are connected to the system but not yet authorized. After receiving its configuration, the authorized access point will immediately be displayed in the above section. For each access point, the list shows:

##### ID

ID of the access point.

##### Label

Label of the AP, which allows it to be identified easily in the network.

##### Channel

Channel the AP transmits on.

##### Group

Access point group the AP is assigned to.

##### MAC

MAC address of the AP.

<input type="checkbox"/>	ID	Label	Channel	Group	MAC	Manage	Accept	Delete
No Records Found								

**Figure 373: Pending Access Points**

#### Rules for Assigning Networks to APs

An access point can only be assigned to a wireless network if the client traffic option of the wireless network and the VLAN tagging option of the access point fit together. The following rules apply:

- Wireless network with client traffic **Separate Zone**: VLAN tagging of the access point can be enabled or disabled.
- Wireless network with client traffic **Bridge to AP LAN**: VLAN tagging of the access point has to be disabled.
- Wireless network with client traffic **Bridge to VLAN**: VLAN tagging of the access point has to be enabled. The respective wireless clients will use the **Bridge to VLAN ID** specified for the wireless network, or they will receive their VLAN ID from the RADIUS server, if specified.



**Note:** An AP 5 can only be assigned to one single wireless network with the **Client traffic** option **Bridge to AP LAN**.

#### Edit Access Point

This page describes how to edit an access point.

1. Go to **Protect > Wireless > Access Points** and click **Edit** icon under the **Manage** column.

2. Specify the Access Point details.

##### ID

Displays the ID for the access point.

#### Label

Specify a label for easier identification of the AP in your network.

#### Country

Select the country where the AP is located.

#### Group

Select to organize APs in groups. If a group has been created before, you can select it from the drop-down list.

ID	A4002666207E8B4
Label	AP100[A4002666207E8B4]
Country	India
Group	None

**Figure 374: Edit Access Point**

- Specify the Wireless Networks details.

#### Wireless Networks

Select the wireless networks that should be broadcasted by the AP.



**Note:** You can only add a wireless network if the AP is not a member of any AP Group.

Wireless Networks *	Add New Item
---------------------	--------------

**Figure 375: Edit Access Point**

- Specify the Mesh Network details.

#### Mesh Networks (*only available for AP50*)

Select the mesh networks that should be broadcasted by the AP.

You can also add APs that should broadcast mesh networks from this page by clicking **Create New**.



**Note:** This option will only be displayed if a mesh network is configured.

- Specify the **Advanced Settings** details.

#### Bridge to Ethernet

Turn it on to bridge the local wireless access point to Ethernet. The existing DHCP server will be used for the bridge port. If a DHCP server does not exist, a new server is automatically created. If you turn it off, the bridge is deleted and all configurations are restored to the physical interface.



**Note:** This feature is available only for IPv4 configurations and applicable only for the SSIDs that are of type, Bridge To LAN.

#### Port to Bridge

Select the port for bridge connection.

-  **Note:** The interface must have an IP address and should not belong to the WAN port or any other bridge. Bridging between VLAN interface and local Wi-Fi is not allowed.

#### Zone

Select the zone for the bridge connection. You cannot select the WAN zone here.

#### Channel 2.4 GHz

Select a channel for your wireless network.

Default: Auto

-  **Note:** Selecting “Auto” will automatically select the least used channel for transmission.

#### Dyn Chan

Enable to scan for the optimal channel at regular intervals. This may result in re-connection of all connected clients.

#### Time-based scan (*available if Dyn Chan is enabled*)

Enable to set a time at which the scan should take place.

#### Select Scan-Time (*available if Time-based scan is enabled*)

Click **Add New Item** and select a scanning time schedule.

#### TX Power

Select the transmission power for the AP.

Default: 100%

#### Channel 5 GHz

Select a channel for your wireless network.

Default: Auto

-  **Note:** Selecting “Auto” will automatically select the least used channel for transmission.

#### Dyn Chan

Enable to scan for the optimal channel at regular intervals. This may result in re-connection of all connected clients.

#### Time-based scan (*available if Dyn Chan is enabled*)

Enable to set a time at which the scan should take place.

#### Select Scan-Time (*available if Time-based scan is enabled*)

Click **Add New Item** and select a scanning time schedule.

#### TX Power 5GHz

Select the transmission power for the AP.

Default: 100%

#### STP

Select **Enabled** to use Spanning Tree protocol (STP). STP prevents bridge loops.

Default: Disabled

#### VLAN Tagging

Select to connect the AP with an existing VLAN Ethernet interface.

Default: Disabled

#### AP VLAN ID (*available if VLAN Tagging is enabled*)

Specify the VLAN ID that will be used by the AP to connect to the device.

The VLAN ID can be any number between 2 and 4094.

Channel 2.4 GHz	<input type="button" value="Auto"/>
Dyn Chan	<input checked="" type="checkbox"/> Enable
Time-based scan	<input checked="" type="checkbox"/> Enable
Select Scan-Time *	<input type="button" value="Add New Item"/>
TX Power	<input type="button" value="100%"/>
Channel 5 GHz	<input type="button" value="Auto"/>
Dyn Chan	<input checked="" type="checkbox"/> Enable
Time-based scan	<input checked="" type="checkbox"/> Enable
Select Scan-Time *	<input type="button" value="Add New Item"/>
TX Power 5GHz	<input type="button" value="100%"/>
STP	<input type="button" value="Disabled"/>
VLAN Tagging	<input type="checkbox"/> Enable

**Figure 376: Edit Access Point**

6. Click Save.

## Access Point Groups

The **Access Point Groups** page allows you to organize access points in groups.

**Protect > Wireless > Access Point Groups** This page provides an overview of all access point groups and Local Wi-Fi Devices. You can add, edit or delete a group. For each group, the list shows:

### Name

Name of the access point group.

### Status

Status of the access point group (active/inactive). Use the toggle switch to enable/disable the access point group.

## Wireless Networks

Wireless networks the access point group is assigned to.

### Access Points

List of all the access points in this group.

<input type="checkbox"/> Name	Status	Wireless Networks	Access Points	Manage
<input type="checkbox"/> DefaultGroup	<input checked="" type="button"/>	Sophos, GuestAP		 

**Figure 377: Access Point Groups**

### Add Access Point Group

This page describes how to add an access point group.

1. Go to **Protect > Wireless > Access Point Groups** and click **Add**.
2. Specify the access point group details.

#### Name

Enter a descriptive name for the new access point group.

#### Wireless Networks

Search for wireless networks and select the wireless networks that should be broadcasted by the access points of this group.



**Note:** For an access point to broadcast a wireless network some conditions have to be fulfilled. They are explained in the chapter [Access Points](#) in the section **Rules for Assigning Networks to APs**.

#### VLAN Tagging

Select **Enable** if you want to activate VLAN tagging.



**Note:** Make sure that the VLAN interface is assigned to the zone which is selected in the **Allowed Zone** list on the **Protect > Wireless > Wireless Settings** page.

#### Access Points

Search for access points and select the ones you want to add to this group.



**Note:** Local Wi-Fi devices cannot be grouped and do not appear in the **Access Point** list. Local Wi-Fi devices appear in the **Access Point Groups** list.

Name *	<input type="text" value="Enter Name"/>
Wireless Networks	<input type="button" value="Add New Item"/>
VLAN Tagging	<input type="checkbox"/> Enable
Access Points	<input type="button" value="Add New Item"/>

**Figure 378: Add Access Point Group**

3. Click **Save**.

## Mesh Networks

The **Mesh Networks** menu allows you to create mesh networks and associate APs.

### Protect > Wireless > Mesh Networks

In a mesh network, multiple access points communicate with each other and broadcast a common wireless network. On the one hand, access points connected via a mesh network can broadcast the same wireless network to clients, thus working as a single access point, while covering a wider area. On the other hand, a mesh network can be used to bridge Ethernet networks without laying cables. Access points associated with a mesh network can play one of two roles: root access point or mesh access point. Both broadcast the mesh network, thus the number of other wireless networks they can broadcast is reduced by one.

#### Root access point

This has a wired connection to Sophos XG Firewall and provides a mesh network. An access point can be root access point for multiple mesh networks.

#### Mesh access point

This needs a mesh network to connect to Sophos XG Firewall via a root access point. An access point can be mesh access point for only one mesh network at a time.

A mesh network can be used to implement a wireless bridge or a wireless repeater:

##### Wireless bridge

Using two access points, you can establish a wireless connection between two Ethernet segments. A wireless bridge is useful when you cannot lay a cable to connect those Ethernet segments. While the first Ethernet segment with your Sophos XG Firewall is connected to the Ethernet interface of the root access point, the second Ethernet segment has to be connected to the Ethernet interface of the mesh access point. Using multiple mesh access points, you can connect more Ethernet segments.



##### Wireless repeater

Your Ethernet with your Sophos XG Firewall is connected to the Ethernet interface of a root access point. The root access point has a wireless connection via the mesh network to a mesh access point, which broadcasts wireless networks to wireless clients.



This page displays a list of all the available mesh networks. You can add, edit or delete a mesh network. For each network the list shows:

#### Mesh-ID

Identifier of the mesh network.

#### Status

Indicates the current status of the mesh network

#### Frequency Band

Frequency band on which the associated access points broadcast the mesh network.

## Related tasks

[Add Mesh Network](#) on page 418

This page describes how to create mesh networks and assign access points to them.

### Add Mesh Network

This page describes how to create mesh networks and assign access points to them.

1. Go to **Protect > Wireless > Mesh Networks** and click **Add**.

2. Specify the **General Settings** details.

#### Mesh ID

Enter a unique ID for the mesh network.

#### Frequency Band

Select a frequency band from the available options:

- 5 GHz
- 2.4 GHz

Access points assigned to this network will transmit the mesh network on the selected frequency band. Generally, it is a good idea to use a different frequency band for the mesh network than for the broadcasted wireless networks.

#### Description

Enter a description or other information to identify the mesh network.

#### Access Point

Select one or more mesh access points.

- a) Click the + icon to select access points that broadcast the mesh network.
- b) Specify the **Mesh Network Role** details.

#### Access Points

Select an access point.



**Note:** Except for AP5 and AP10, all the APs can be used for broadcasting mesh networks.

#### Role

Define the access point's role for the selected mesh network. A root access point is directly connected to Sophos XG Firewall. A mesh access point, after having received its initial configuration, once unplugged from the Sophos XG Firewall will connect to a root access point via the mesh network.



**Note:** An access point can be mesh access point only for one mesh network.

The dialog box has the following fields:

- Mesh-ID \***: An input field.
- Frequency Band**: A dropdown menu set to **5 GHz**.
- Description**: An input field.
- Access Points**: An input field.
- Search / Add**: A button with a plus sign (+).

**Figure 379: Add Mesh Network**

- c) Click **Save**.

The dialog window is closed and the access point is added to the **Access Points** list.



**Note:** It is crucial for the initial configuration to plug the mesh access point, like every other access point, into one of the Ethernet segments selected in the **Allowed Zone** box on the **Protect > Wireless > Wireless** page.

3. Click **Save**.

## Hotspots

The **Hotspots** menu allows you to enable the Hotspots feature and define users who are allowed to view and distribute hotspot access information.

### Protect > Wireless > Hotspots

By means of hotspots caf  s, hotels, companies, etc. can provide time- and traffic-restricted Internet access to guests. The hotspot feature is available within the Wireless Protection subscription, but also works with wired networks.



**Note:** You can also view and manage the hotspot status on the **Monitor & Analyze > Diagnostics > Services** page.

### Hotspot Generation

In the first step, the administrator creates and enables a hotspot with a specific type of access. The following types are available:

- **Terms of use acceptance**: The guest is presented with terms of use, which you can define, and has to select a checkbox to get access.
- **Password of the day**: The guest has to enter a password to get access. The password changes on a daily basis.
- **Voucher**: The guest gets a voucher and has to enter the voucher code to get access. The voucher can be limited in the number of devices, in time, and traffic.

### Distribution of Access Information to Guests

With the access types **Password of the day** and **Voucher**, the access information has to be handed out to the guests. Therefore you can define users who are allowed to manage and distribute access information. Those users receive and distribute the access information via the **Hotspot** tab of the User Portal:

- **Password of the day**: The current password can be sent via email and the users find the password in the User Portal. The users forward the password to the guests. They can generate or enter a new password. The former password automatically becomes invalid and active sessions will be terminated. Other potential users will be informed of the new password, either by email or via the User Portal, depending on what is configured for them.

- **Voucher:** In the User Portal, users can create vouchers, each with a unique code. Different types of vouchers can be available if specified by the administrator. The vouchers can be printed or exported and given to the guests. A list of created vouchers gives an overview of their usage and helps to manage them.

## Legal Information

In many countries, operating a public wireless LAN is subject to specific national laws, restricting access to websites of legally questionable content (e.g., file sharing sites, extremist websites, etc.). To meet this requirement, you can combine the hotspot with the web protection capabilities of Sophos XG Firewall which empowers you to control web access by blocking or allowing a single URL to an entire website category type. Sophos XG Firewall puts you in control of who accesses what and when. That way you can restrict hotspot usage as national or corporate policies require you to. In addition, the current feature of Sophos XG Firewall permits advanced logging and reporting capabilities. Reporting tracks who visited which site, when, and how many times, allowing you to identify inappropriate usage in case you want to operate a hotspot without any access restrictions. Which is even more important if legal regulations require you to register your hotspot at the national's regulatory body.

For each hotspot, the list shows:

### Name

Displays the name of the hotspot.

### Hotspot Type

Displays the type of the hotspot.

-  **Note:** If you have configured direct proxy settings within your web browser and using Hotspot, you need to add Device's IP in the proxy exception list.

### Related concepts

[Hotspot Voucher Definition](#) on page 428

Hotspot voucher definitions specify network access. You can use voucher definitions to limit the validity period, time quota, and data volume for users who have access to voucher-type hotspots.

### Related tasks

[Add Hotspot](#) on page 420

This page describes how to add a hotspot.

### Add Hotspot

This page describes how to add a hotspot.

-  **Note:** A hotspot has to be assigned to an existing interface, typically a WLAN interface. All hosts using this interface will automatically be restricted by the hotspot. Therefore, before you create a hotspot you would typically create a wireless network with client traffic **Separate Zone**, then create an interface for the respective WLAN interface hardware.

1. Go to **Protect > Wireless > Hotspots** and click **Add**.

2. Specify the followings:

#### Name

Enter a unique name for the hotspot.

#### Description

Enter a description or other information to identify the Hotspot.

#### Interfaces

Select or add the interfaces which are to be restricted by the hotspot. An interface can only be used by one hotspot.

-  **Note:** Hotspots will work only on LAN and DMZ member interfaces of the bridge.

You should not select an uplink interface here because traffic to the Internet will be completely blocked afterwards. Additionally, we strongly advise not to use interfaces

applied by servers which provide essential services like authentication. You may irreversibly lock yourself out of Sophos XG Firewall.

### **Application Filter Policy**

Select or add an application filter policy for the hotspot.

### **Web Policy**

Select or add a web policy for the hotspot.

### **IPS Policy**

Select or add IPS policy for the hotspot.

### **Traffic Shaping Policy**

Select or add a traffic shaping policy for the hotspot.

### **Redirect to HTTPS**

Enable this option to redirect users to HTTPS.

#### **Hostname Type (*available only if Redirect to HTTPS is enabled*)**

Select the hostname type for the hotspot.

Available Options:

- None (IP Address)
- Custom hostname

#### **Hostname (*available only if Custom hostname is selected*)**

Add a hostname for the redirection.

### **Hotspot Type**

Select a hotspot type for the selected interfaces.

- **Terms of Use Acceptance** - Customers can access the Internet after accepting the terms of use.  
**Session Expires**

Select the time span after which the access will be denied. After that, with the hotspot type **Terms of Use Acceptance**, the users have to accept the terms of use again to log in.

#### **Terms of Use**

Add the text to be displayed as terms of use. Simple HTML markup and hyperlinks are allowed.

- **Password of the Day** - A new password will be created automatically once a day. This password will be available in the User Portal on the Hotspots tab which is available to all users specified for this hotspot. Additionally it will be sent to the specified email address(es).

#### **Password Creation Time**

Select the time of the day at which the new password will be created. At this time the former password will immediately become invalid and current sessions will be terminated.

#### **Send Password by email to**

Add email addresses to which the password will be sent.

#### **Synchronize password with PSK of wireless networks**

Select this option to synchronize the new generated/saved password with wireless PSK.



**Note:** With the new PSK all APs that are configured with a separate zone wireless network that is also used as a hotspot interface will be reconfigured and restarted. This means all connections will be dropped.

### **Administrative Users**

Select or add users for administrative settings. Administrative users are allowed to create vouchers or change the password of the day in the User Portal. By default nobody is allowed to enter administrative settings.

- **Voucher** With this hotspot type, tokens with different limitations and properties can be generated in the User Portal, printed and given to customers. After entering the code, the customers can then access the Internet directly.

#### **Voucher Definitions**

Add or select the voucher definitions you want to use for the hotspot. How to add a voucher definition is explained on the **Add Hotspot Voucher** page.

#### **Devices per voucher**

Enter the number of devices which are allowed to log in with one voucher during its lifetime. It is not recommended to use the “unlimited” option.

#### **Administrative Users**

Select or add users for administrative settings. Administrative users are allowed to create vouchers or change the password of the day in the User Portal. By default nobody is allowed to enter administrative settings.

#### **Users Have to Accept Terms of Use (*not available with hotspot type Terms of Use Acceptance*)**

Enable this option if you want the hotspot users to accept your terms of use before accessing the Internet.

#### **Terms of Use**

Add the text to be displayed as terms of use. Simple HTML markup and hyperlinks are allowed.

#### **Redirect to URL after login**

Enable this so that users will be redirected automatically to a particular URL after entering password or voucher data. The URL could, for example, be your hotel’s website or a web page stating your portal system policies.

#### **URL**

Enter the URL to which the user will be redirected .

Name *	<input type="text"/>
Description	<input type="text"/>
Interfaces *	<input type="text"/>  <a href="#">Add New Item</a>
Application Filter Policy	<input type="text"/> None ▾
Web Policy	<input type="text"/> None ▾
IPS Policy	<input type="text"/> None ▾
Traffic Shaping Policy	<input type="text"/> None ▾
Redirect to HTTPS	<input type="checkbox"/> OFF
Hotspot type	<input type="text"/> Terms of Use Acceptance ▾
Session expires	<input type="text"/> After 2 hours ▾
Terms of use *	<input type="text"/>

### 3. Specify the **Hotspot Customization** details.

#### **Enable Customization**

Enable to use a customized HTML file with your own images and stylesheets. Additionally, you can customize the voucher layout.

#### **Customization Type**

Select the customization type.

- **Basic** Uses the default login page template. If required, change logo, title, and text.

##### **Logo**

Upload a logo for the login page. Supported image file types are jpg, jpeg, png and gif. A maximum image width of 300 px and height of 100 px is recommended (depending on the title length).

##### **Scale logo to recommended size**

If selected, a logo exceeding the recommended width or height will be scaled down and displayed in the recommended size. If it is not selected, the logo will be displayed in the original size.

##### **Title**

Add a title for the login page. Simple HTML markup and hyperlinks are allowed.

##### **Custom Text**

Add additional text for the login page. You can, for example, enter the SSID of the wireless network to be used. Simple HTML markup and hyperlinks are allowed.

- **Full** Select an individual login HTML page.

##### **Login Page Template**

Select the HTML template you want to use for your individual login page. Browse to select and upload the file. In this template, you can use variables that can insert information for each hotspot dynamically. For example, you can add the company name and administrator information, the terms of use and the login form. See detailed information in the chapter **Login Page Template**.

##### **Images/Stylesheet**

Add files that are referenced in your login page template, e.g., images, stylesheets, or JavaScript files. Browse to select and upload the files.

#### **Voucher Template (*only available for the hotspot type Voucher*)**

Browse to select and upload a PDF file with the voucher layout. By default, a default template is used. The voucher PDF file has to be of PDF version PDF 1.5 or lower. It may have any page size and format—both size and format will be adjusted during voucher creation in the User Portal, depending on page size and number of vouchers per page specified there.

The PDF file may contain the following variables that will be replaced with the respective values during voucher generation in the User Portal:

- Wireless network name (SSID): <?ssid0?> (and <?ssid1?>, <?ssid2?> and so on, if the WLAN has more than one SSIDs)
- Wireless network password: <?psk0?> (and <?psk1?>, <?psk2?> and so on, if the WLAN has more than one SSIDs)
- Voucher code: <?code?>
- Voucher validity time: <?validity?>
- Voucher data limit: <?datalimit?>
- Voucher time limit: <?timelimit?>
- Comment: <?comment?>
- QR code with the hotspot access data encoded: <?qrX?>. The upper left corner of the QR code will be placed on the lower left corner of the variable.



**Note:** When using variables, the PDF file must include the entire character sets of the fonts used. When a variable is replaced by its value, and one of the substitute characters is not available, it

will be displayed incorrectly. We recommend to add the string <? abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789?> (for English usage) to your PDF file, which will be removed automatically during voucher generation. If you use another language, you can include any other character set you want. Additionally, we recommend to use a separate line for the variables as the layout could get corrupted if the substituted text is too long.

The screenshot shows a configuration interface for hotspot customization. It includes the following fields:

- Enable Customization:** A toggle switch set to **ON**.
- Customization Type:** A dropdown menu set to **Basic**.
- Logo:** A field with a **Browse...** button and the message **No file selected.**
- Scale logo to recommended size:** A toggle switch set to **OFF**.
- Title:** An empty text input field.
- Custom Text:** A large empty text input field with a small icon in the bottom right corner.

**Figure 380: Hotspot Customization**

#### 4. Click Save.

You can see if the hotspot is running on the **Configure > System Services > Services** page. There you can also stop or start the hotspot.

#### Related concepts

[Services](#) on page 301

**Services** page allows you to view and manage the status of configured services.

[Login Page Template](#) on page 425

This page gives an overview of possible variables of the hotspot login template.

#### Related tasks

[Add Hotspot Voucher Definition](#) on page 428

Create a voucher definition.

#### Login Page Template

This page gives an overview of possible variables of the hotspot login template.

The HTML template for the login page may contain various variables that can insert information for the hotspot login page dynamically. When the device processes a template in order to display a login page, it replaces any template variables with the relevant value.

#### General variables

- <?company\_text?:>: Default company text
- <?company\_logo?:>: Default company logo (Sophos logo). The variable will be replaced by the path of the logo file, usage e.g., 
- <?admin\_contact?:>: Administrator name or address as defined on **System > Administration > Notification Settings** (**Send Notifications to Email Address** field)

- <?admin\_message?>: Administrator information label (default: For administrative questions please contact:)
- <?error?>: Error message that arose while trying to log in.

### Variables used for all hotspot types

- <?terms?>: Terms of use (as defined on the **Add Hotspot** page)
- <?redirect\_host?>: Redirect URL that is specified for the hotspot (as defined on the **Add Hotspot** page)
- <?location?>: URL the user requested
- <?location\_host?>: Hostname of the URL the user requested
- <?login\_form?>: Login form suitable for the respective hotspot type: **Password** text box, **Token** text box, **Username** and **Password** text boxes, or **Accept** checkbox, and **Login** button.



**Note:** For creating customized login forms, see section *User Specific Login Form* below.

- <?asset\_path?> (only important for customization mode **Full**): Hotspot specific directory for storage of images or stylesheets (example usage: )

### Variables only used for hotspot type Voucher

- <?maclimit?> Number of allowed devices per voucher of this hotspot (as defined on the **Add Hotspot** page)
- <?numdevices?>: Number of devices used for this voucher
- <?timeend?>: Validity period (as defined on the **Add Hotspot Voucher** page)
- <?time\_total?>: Total time quota allowed (as defined on the **Add Hotspot Voucher** page)
- <?traffic\_total?>: Total data volume allowed (as defined on the **Add Hotspot Voucher** page)

Templates can contain `if` variables that make up sections like the ones shown below. Each section has an opening and a closing variable. The contents of an `if` section is only displayed on a specific condition.

If Section	Meaning
<?if_loggedin?> <?if_loggedin_end? >	Section is displayed when the user has successfully logged in.
<?if_notloggedin?> <? if_notloggedin_end? >	Section is displayed when the user has not yet logged in, e.g., because terms of use have to be accepted or because an error occurred.
<? if_authtype_password? > <? if_authtype_password_end? >	Section is displayed when hotspot type is <b>Password of the Day</b> .
<? if_authtype_disclaimer? > <? if_authtype_disclaimer_end? >	Section is displayed when hotspot type is <b>Terms of Use Acceptance</b> .

If Section	Meaning
<? if_authtype_token?> <? if_authtype_token_end?>	Section is displayed when hotspot type is <b>Voucher</b> .
<?if_location?> <?if_location_end?>	Section is displayed when the user has been redirected.
<?if_redirect_url?> <? if_redirect_url_end?>	Section is displayed when the checkbox <b>Redirect to URL After Login</b> is enabled.
<? if_not_redirect_url?> <? if_not_redirect_url_end?>	Section is displayed when the checkbox <b>Redirect to URL after login</b> is disabled.
<?if_timelimit?> <?if_timelimit_end?>	Section is displayed when a validity period is set for a voucher.
<?if_trafficlimit?> <? if_trafficlimit_end?>	Section is displayed when a data volume is set for a voucher.
<?if_timequota?> <?if_timequota_end?>	Section is displayed when a time quota is set for a voucher.
<?if_maclimit?> <?if_maclimit_end?>	Section is displayed when a <b>Devices per voucher</b> value is specified.
<?if_terms?> <?if_terms_end?>	Section is displayed when <b>Terms of Use</b> are defined and enabled.
<?if_error?> <?if_error_end?>	Section is displayed when an error occurred while trying to log in.

### User-Specific Login Form

If you want to create your own login form instead of using the pre-defined <?login\_form?> variable, consider the following:

- Enclose the form in the following tags:  

```
<form action="?action=login" method="POST"> ... </form>
```
- For a **Terms of Use Acceptance** hotspot, add a checkbox named "accept":

- ```
<input type="checkbox" name="accept">
• For Password of the Day or Voucher hotspots, add a text box named "token":
<input type="text" name="token">
• Add a means to submit the form, e.g., a "Login" button:
<input type="submit" name="login" value="Login">
```

## Hotspot Voucher Definition

Hotspot voucher definitions specify network access. You can use voucher definitions to limit the validity period, time quota, and data volume for users who have access to voucher-type hotspots.

### Related concepts

[Hotspot Settings](#) on page 432

The **Hotspot Settings** page allows you to make additional hotspot settings.

### Related tasks

[Add Hotspot Voucher Definition](#) on page 428

Create a voucher definition.

### Add Hotspot Voucher Definition

Create a voucher definition.

1. Go to **Protect > Wireless > Hotspot Voucher Definition** and click **Add**.
2. Specify the voucher definition details.

#### Name

Specify a descriptive name for the voucher definition.

#### Description

Specify a description or other information.

#### Validity period

Specify the time for which vouchers of this type will be valid. The validity period starts from the first login.

Acceptable range: 1 minute to 730 days

#### Time quota

Specify the maximum connectivity time for vouchers of this type. The time quota starts at login and stops at logout. Counting stops after 5 minutes of inactivity.

Acceptable range: 1 minute to 500 hours

#### Data volume

Specify the maximum volume of data to be transmitted for vouchers of this type.

Acceptable range: 1 MB to 100 GB

The form consists of five input fields arranged in two rows. The first row contains 'Name \*' with a text input field, and 'Description' with a large text area. The second row contains 'Validity period \*' with a text input field and a dropdown menu set to 'Minutes', and 'Time quota' with a text input field and a dropdown menu set to 'Minutes'. Below these is another row with 'Data volume' and a text input field, followed by a dropdown menu set to 'MB'.

**Figure 381: Add Hotspot Voucher**

3. Click Save.

## Rogue AP Scan

This section is applicable to Wi-Fi models only.

A Rogue Access Point (AP) is any Wi-Fi access point connected to your network without authorization. It can be a setup used by an attacker for the purpose of sniffing wireless network traffic and can be used to conduct a man-in-the-middle attack. It allows anyone with a Wi-Fi-equipped device to connect to your corporate network, leaving your IT assets wide open for the casual snooper or criminal hacker.

Device can alleviate this by recognizing rogue access points potentially attempting to gain access to your network.

### General Settings

Click **Schedule system-triggered scan** to enable a scheduled scan to discover authorized APs and rogue APs. You can select from the pre-defined schedules or create a custom schedule from **System > Profiles > Schedule**.

The interface includes a checkbox labeled 'Schedule system-triggered scan at', a dropdown menu labeled 'Schedule' with a small info icon, and a large blue 'Apply' button at the bottom.

**Figure 382: General Settings**

### Discover Access Points

To increase the security capabilities and identify unauthorized APs, Sophos Wireless Devices provide scanning capability by which nearby APs can be discovered and an administrator can take countermeasures against the most common types of illicit wireless activity.

To manually scan for the automatic discovery of APs, click **Scan Now**.

All the Access Points discovered are regarded as unrecognized until they are identified as authorized or rogue. To authorize an access point, click the icon against it in the Unrecognized AP table. To mark an access point as rogue, click the icon against it in the Unrecognized AP table.

If you are scanning for the first time after enabling Wireless LAN, all the discovered APs will be listed in the **Unrecognized Access Points** table. The scanning result is displayed in the form of 3 tables:

### Unrecognized Access Points table

The table lists all the nearby APs discovered and displays the following information:  
**Channel**

The radio channel used by the access point.

#### **BSSID**

The MAC Address of the radio interface of the detected access point.

#### **SSID**

The radio SSID of the access point.

#### **Signal Strength**

The strength of the detected radio signal

#### **Security Mode**

Mode for encrypting the wireless traffic

#### **Wireless Mode**

Wireless protocol

#### **Action**

Click the icon  to mark the AP as an authorized AP and move it to the Authorized AP table. Click the icon  to mark the AP as a rogue AP and move it to the Rogue AP table.

Channel	BSSID	SSID	Signal Strength	Security Mode	Wireless Mode	Action
1	74:EA:3A:A7:E4:D9		62	WEP	11b/g	 

**Figure 383: Unrecognized Access Points**

#### **Rogue Access Points table**

The table lists all the APs marked as “Rogue” and displays the following information:

#### **Channel**

The radio channel used by the access point.

#### **BSSID**

The MAC Address of the radio interface of the detected access point.

#### **SSID**

The radio SSID of the access point.

#### **Signal Strength**

The strength of the detected radio signal

#### **Security Mode**

Mode for encrypting the wireless traffic

#### **Wireless Mode**

Wireless protocol

#### **Action**

Click the icon  to mark the AP as an authorized AP and move it to the Authorized AP table. Click the icon  to mark the AP as an unrecognized AP and move it to the Unrecognized AP table.

Channel	BSSID	SSID	Signal Strength	Security Mode	Wireless Mode	Action
No Records Found						

**Figure 384: Rogue Access Points**

#### **Authorized Access Points table**

The table lists all the APs marked as “Authorized” and displays the following information:

#### **Channel**

The radio channel used by the access point.

#### **BSSID**

The MAC Address of the radio interface of the detected access point.

#### **SSID**

The radio SSID of the access point.

#### **Signal Strength**

The strength of the detected radio signal

#### **Security Mode**

Mode for encrypting the wireless traffic

#### **Wireless Mode**

Wireless protocol

#### **Action**

Click the icon  to mark the AP as an unrecognized AP and move it to the Unrecognized AP table.

Click the icon  to mark the AP as a rogue AP and move it to the Rogue AP table.

Channel	BSSID	SSID	Signal Strength	Security Mode	Wireless Mode	Action
No Records Found						

**Figure 385: Authorized Access Points**

## **Wireless Settings**

The Wireless Settings page allows general configuration of wireless networks.

1. Go to **Protect > Wireless > Wireless Settings**.
2. Specify the **Global Settings**.

#### **Enable Wireless Protection**

Click the toggle switch to enable Wireless Protection.

#### **Allowed Zone**

Select network zones that are to be allowed for access point connectivity. These are the zones where access points are deployed to.

 **Note:** If the wireless network uses WPA/WPA2 Enterprise Authentication as encryption mode then a RADIUS server needs to be specified.

Enable Wireless Protection	<input checked="" type="checkbox"/>
Allowed Zone	<input type="button" value="Add New Item"/>

**Figure 386: Global Settings**

3. Specify the **Advanced Settings**.

#### **Notification Timeout**

If an access point goes offline you get a notification. The **Notification Timeout** lets you configure a timeout for the notification. This means, if you set a delay of 2 minutes, the notification will be sent only if the access point is offline for at least 2 minutes. After the specified time, the AP will be considered inactive.

#### Timeout (in minutes)

The notification timeout requires an integer.

Default: 5 minutes.

#### Enterprise Authentication

For enterprise authentication, you need to provide some information of your RADIUS server. Note that access points do not communicate with the RADIUS server for authentication but only the Sophos Firewall OS. Port 414 is used for the RADIUS communication between the Sophos Firewall OS and the access points.

#### RADIUS Server

Select the required RADIUS server from the drop-down list. Servers can be added and configured on **Configure > Authentication > Servers**.

 **Note:** When your RADIUS server is connected to the Sophos Firewall OS via an IPsec tunnel, you have to configure an additional SNAT rule to ensure that the communication works correctly. On the **System > Profiles > Network Address Translation** page, add the following SNAT rule: For traffic from the APs' network(s), using service RADIUS, and going to the RADIUS server, replace the source address with the IP address of Sophos Firewall OS used to reach the RADIUS server.



The screenshot shows a configuration interface with two main sections. The first section, 'Notification Timeout', contains a field labeled 'Timeout (in minutes)' with a value of '5'. The second section, 'Enterprise Authentication', contains a dropdown menu labeled 'RADIUS Server' with the option 'None' selected.

**Figure 387: Advanced Settings**

- Click **Apply**.

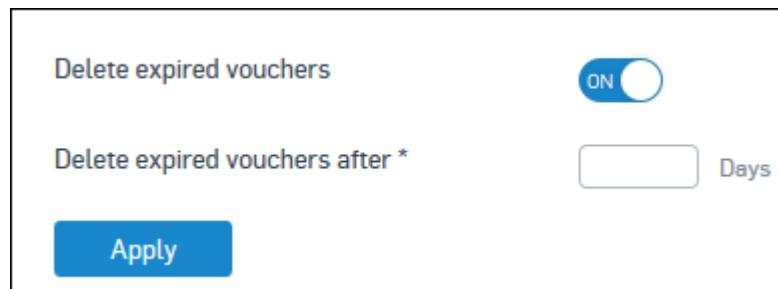
#### Hotspot Settings

The **Hotspot Settings** page allows you to make additional hotspot settings.

Use this page to configure additional hotspot settings.

#### General Voucher Options

Here you can decide if and after which time interval you want to delete expired vouchers from the database. In the hotspot log you will still find information about deleted vouchers.



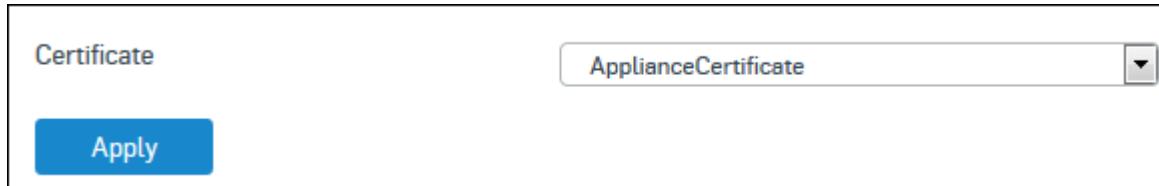
The screenshot shows a configuration interface for general voucher options. It features a toggle switch labeled 'Delete expired vouchers' which is turned 'ON'. Below the switch is a text input field labeled 'Delete expired vouchers after \*' with a placeholder 'Days'. At the bottom is a blue 'Apply' button.

**Figure 388: General Voucher Options**

## Login Page Certificate

You can generate or upload new certificates on the **System > Certificates > Certificates** page.

Select the requested certificate from the drop-down list and click **Apply** to activate it.



**Figure 389: Login Page Certificate**

## Walled Garden

Add or select specific hosts or networks which ought to be permanently accessible to all users, without the need of entering a password or a voucher code.

You can add a new IP host, MAC host or FQDN host directly from this page or via the **System > Hosts and Services** menu.



**Figure 390: Walled Garden**

## Download Templates

Here you can download the hotspot login template and the voucher template that are to be used by default when adding a new hotspot. You can modify the default templates to customize your hotspot login page or the voucher design without the need to create them from scratch.

You can upload a customized HTML and PDF template when editing or adding a template on the **Protect > Wireless > Hotspots** page in the section **Hotspot Customization** (upload is available only if the customization type **Full** is selected).



**Figure 391: Download Templates**

## Email

---

**This feature requires a subscription. It can be configured but cannot be enforced without a valid Email Protection subscription.**

From the Email tab, you can configure SMTP/S, POP/S and IMAP/S settings, Email Security Policies, Secure PDF eXchange (SPX) and Data Control.

The device offers comprehensive Email Security, preventing sophisticated forms of zero-hour threats and blended attacks involving spam, botnets, phishing, spyware and more. The basic email protection configuration includes:

- Creating policies to allow or deny email traffic to and from your Email Server.
- Apply Spam, Malware, Data and File protection on email traffic.
- SPX
- configuring an email threshold size for scanning
- specifying action to be taken if a virus is detected
- blocking mails based on sender or recipient
- blocking mails with certain file types.

### **SMTP Deployment Modes**

SF can be deployed in Two (2) Modes:

- Legacy Mode
- MTA Mode

#### **Legacy Mode**

In Legacy Mode, SF acts as a transparent proxy that scans emails for malware and spam, applies SPX Encryption and Data Protection. Refer to the following guides to see how SF can be configured to scan email traffic in Legacy Mode:

#### **MTA Mode**

In MTA Mode, SF acts as a Mail Transfer Agent. A Mail Transfer Agent (MTA) is a service that is responsible for receiving and routing emails to their specified destinations.

Deploy SF in MTA Mode when you want it to perform actual routing of emails as compared to Legacy Mode where SF only forwards the email traffic as a proxy.

In MTA Mode, SF performs the following functions:

- Performs relaying and routing of emails. You can configure relaying of emails from **Email > Relay Settings**.
- Protects multiple Email Servers using SMTP Policies. From **Email > Policies > SMTP Policies**, you define the kind of protection you want to apply on each of your Email Domains.
- Displays email messages that are either waiting or failed to be delivered in the **Email > Mail Spool**.
- Displays logs for all the emails processed by the Device from **Email > Mail Logs**.

### **MTA Mode**

#### **Policies**

**This feature requires a subscription. It can be configured but cannot be enforced without a valid Email Protection subscription.**

This page allows configuration of SMTP Route and Scan Policies, SMTP Malware Scan Policies, SMTP Spam Scan Policies and POP-IMAP Scan Policies:

- SMTP Route and Scan Policies (MTA Mode)
- SMTP Malware Scan Policies (Legacy Mode)
- SMTP Spam Scan Policies (Legacy Mode)
- POP3-IMAP Scan Policies (MTA and Legacy Mode)

#### **SMTP Route and Scan Policies**

**SMTP Route and Scan policies appear only when MTA (Mail Transfer Agent) mode is enabled. MTA mode is available only in Sophos Firewall XG105, Cyberoam CR25iNG, Sophos UTM SG105, and higher models.**

Device allows you to create SMTP Route and Scan policies which can be used to protect multiple Domains on your internal Email Server(s). Using these policies, device protects the server(s) from remote attacks and additionally provide powerful virus scanning, email encryption and email filtering services.

Click **Add Policy** and then **SMTP Route & Scan** to add a new policy. To update an existing policy, click the desired policy.

### **SMTP Malware Scan Policies**

**SMTP Malware Scan policies appear only when Legacy mode is enabled. The device acts as a transparent proxy.**

SMTP Malware Scan policies allow you to define action to be taken on emails if they are virus-infected or contain a protected attachment. Based on the action defined in rule, such emails can be delivered as they are, dropped, or cleaned and then delivered or quarantined.

A Malware Scan policy defines:

- whether to quarantine the email
- whether sender, receiver or administrator are to be notified
- whether to block the email containing a specified file type
- what action is to be taken if email is infected or contains a protected attachment: deliver as it is, drop, clean and then deliver

 **Note:** You can also view the Quarantine from **Protect > Email > SMTP Quarantine** page.

A default SMTP Malware Scan policy named **default-smtp-av** is pre-configured in the device and applied to all SMTP traffic as soon as you subscribe to the Email Protection Module. We recommend that you create separate rules fine-tuned to your specific network requirements to minimize the possibility of threats.

Click **Add Policy** and then **SMTP Malware Scan** to add a new policy. To update an existing policy, click the desired policy.

### **SMTP Spam Scan and POP-IMAP Scan Policies**

**SMTP Spam Scan policies appear only when Legacy mode is enabled.**

**POP-IMAP Scan policy is available in both MTA and Legacy modes.**

When you subscribe to the Email Protection Module, SMTP Spam Scan and POP-IMAP Scan policies can be configured for particular senders and recipients.

A policy defines the action to be taken if an email is detected as Spam, Probable Spam, part of Virus Outbreak or Probable Virus Outbreak.

To reduce the risk of losing legitimate messages, the Spam Quarantine repository (a storage location) provides administrators with a way to automatically quarantine emails that are identified as spam. This helps in managing spam and probable spam quarantined mails so that the user can take appropriate actions on such emails.

A default POP-IMAP Scan policy named **default-pop-av** is pre-configured in the device and applied to all POP3/S and IMAP/S traffic so that whenever a virus gets detected in an email, the virus-affected attachment is stripped from the email and the email body is replaced with a notification message.

#### **Detection of Spam attributes**

The device uses Content Filtering, and premium and standard Realtime Blackhole Lists (RBLs) to check for the spam attributes in SMTP/S, POP3/S and IMAP/S emails:

- Premium
- Standard

RBL is a list of IP Addresses whose owners refuse to stop the proliferation of spam, that is, owners who are responsible for spam or are hijacked for spam relay. The device checks each RBL for the connecting IP Address. If the IP Address matches one on the list, then the specified action in the policy is taken.

#### **Add SMTP Route and Scan Policy**

**SMTP Route and Scan policies appear only when MTA (Mail Transfer Agent) mode is enabled. MTA mode is available only in Sophos Firewall XG105, Cyberoam CR25iNG, Sophos UTM SG105, and higher models.**

**This feature requires a subscription. It can be configured but cannot be enforced without a valid Email Protection subscription.**

SMTP route and scan policy allows you to protect emails from spam and malware, to SPX-encrypt emails and to provide data and file protection.

1. Go to **Protect > Email > Policies** and click **Add Policy**. Click **SMTP Route & Scan**.
2. Enter the **Name**.
3. Enter the **Domains and Routing Target** details.

#### Protected Domain

Select the domains. The policy applies to emails to and from the selected domains. To add a new domain, click **Create New**.

Emails received by users of the protected domains are **Inbound Emails**.

Emails sent out by users of the protected domains are **Outbound Emails**.

Emails sent among users of protected domains are **Internal Emails**.

#### Route By

Select the email server to forward the emails to. Select from the following server types:

#### Available Options:

**Static Host:** From the **Host List**, select the static IP addresses of the internal email servers. If the first host in the selected list is not reachable, the device forwards emails to the next host until it reaches the end of the list. To create a new host, click **Create**.  
**MX:** Select to route emails based on MX records.

#### Global Action

Select the action.  
**Accept:** Accepts all emails to the specified domains. You can apply SPX encryption on outbound emails by selecting the **SPX Template** from the drop-down list.  
**Reject:** Rejects all emails to the specified domains. Sender is notified.

The screenshot shows the 'Domains And Routing Target' configuration page. It includes fields for 'Protected Domain' (with an 'Add New Item' button), 'Global Action' (set to 'Accept'), 'SPX Template' (set to 'None'), and 'Route By' (set to 'MX').

**Figure 392: Domains and Routing Target**

4. Turn on **Spam Protection**.

You can enable protection for inbound and outbound spam, virus outbreak and blacklisted sender IP addresses through RBLs. Greylisting allows the device to control spam. When greylisting, the device temporarily rejects inbound emails from IP addresses of unknown email servers for a five-minute period. Subsequent to this period, legitimate email servers retry sending rejected emails at regular intervals. The device accepts the re-sent emails and greylists the sender's IP address for a specific period. Recipient verification is the process of checking the recipients of an inbound email to one of your Internal mail server. Recipient email address in the message envelope is checked against the email user account on the destination mail server. Mails to non-existent users are rejected. If the mail server is not reachable within the defined timeout period of 90 seconds, the recipient is accepted. This reduces the load on the firewall as it will only process mail for valid recipients and conserve quarantine space.

Turning off recipient verification is not recommended as it might lead to higher spam mails and clogging of quarantine space.

#### Available Actions:

- **None**
- **Warn:** Delivers the email to the recipient after adding a prefix to the subject. Specify the prefix in **Prefix Subject**.
- **Quarantine**
- **Drop:** Drops the email without sending a notification to the sender.

Default: Drop

**Figure 393: Spam Protection**

5. Turn on **Malware Protection**.

#### Scanning

Select the scanning action.

#### Available Actions:

**Disable:** Emails are not scanned. **Enable:** Emails are scanned by the device's anti-virus engine.



#### Note:

In Sophos Firewall XG105, Cyberoam CR500iNG, and Sophos UTM SG105, and higher models, **Enable** is replaced by the following options.

**Single Anti-Virus:** The primary anti-virus engine scans the emails.

**Dual Anti-Virus:** The primary and secondary engines scan emails sequentially.

Select the **Primary Anti-Virus Engine** from **Protect > Email > General Settings > Malware Protection**.

#### Detect zero-day threats with Sandstorm (Sandstorm Module required)

Enable to send emails for Sandstorm analysis. Emails found clean by Sandstorm will be delivered to the recipient(s) while selected action will be applied on those found malicious.



**Note:** Cannot implement Sandstorm with Single Anti-Virus Scanning, if Avira is the Primary Anti-Virus Engine. You can update it from **Protect > General Settings > Malware Protection** or **Configure > Configure > System Services > Malware Protection**.

### Scanned File Size (available if Detect zero-day threats with Sandstorm is enabled)

Enter the size of files that can be analyzed by Sandstorm. Files with size greater than that will not be analyzed.

### Anti-virus Action

Select the action to be taken against malicious emails.

#### Available Actions:

- **None**
- **Warn:** Delivers the email to the recipient after adding a prefix to the subject. Specify the prefix in **Prefix Subject**.
- **Quarantine**
- **Drop:** Drops the email without sending a notification to the sender.

### Notify Sender

Select to notify the sender about the infected email.

### Quarantine unscannable content

Select to quarantine emails that could not be scanned. These include corrupt, encrypted, compressed files, oversized emails, and emails not scanned due to an internal error.

**Figure 394: Malware Protection**

- Turn on **File Protection** to filter specific attachments.

### Block File Types

Select the type of attachments you want to block. The corresponding MIME headers populate the **MIME Whitelist**.

To select more than one file type, press Ctrl+Shift.

The device contains a default list of file types with the relevant file extensions.

Refer to **Email > ... > File Type** to view the list of file extensions.

Select **All** to block emails with an attachment.

Select **None** to allow emails with an attachment.

### MIME White List

Select the MIME headers to be allowed during the malware scan. Unselected headers are blocked.

### Drop Message Greater Than

Enter the maximum file size (in KB) to be scanned by the device. Larger emails are dropped.

Default: 51200 KB



**Figure 395: File Protection**

- Turn on **Data Protection**. (applicable only to outbound emails)

#### Data Control List

Select the list to be applied to scan emails for sensitive information.

Data Control Lists (DCL) can be created from the pre-configured Sophos Content Control List (CCL), which provides common financial and personally identifiable data types, like credit card numbers, social security numbers, postal addresses, or email addresses.

You can create a list from **Protect > Email > Data Control List**.

#### Data Control List Action

Select the action to be taken against emails containing sensitive information.

##### Available Actions:

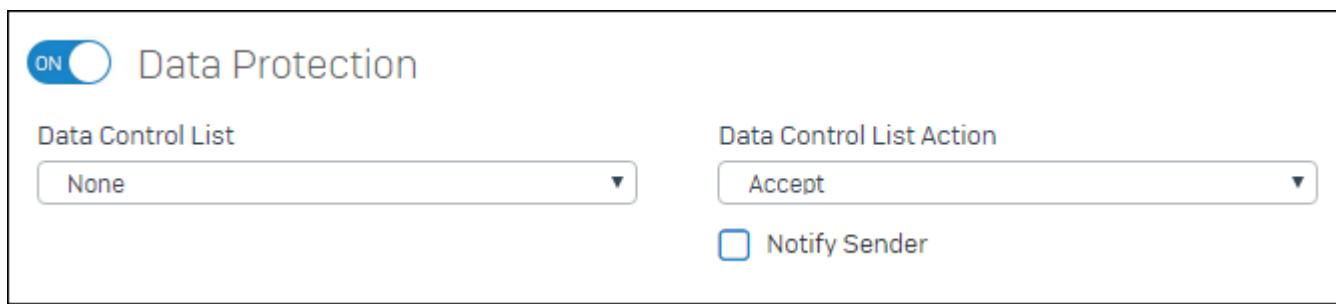
**Accept:** Accepts the email and delivers it to the recipient.

**Accept with SPX:** Accepts and SPX-encrypts the email before delivering it to the recipient. Select the **SPX Template** to be applied to the email. You can create **SPX Templates** from **Protect > Email > Encryption**.

**Drop:** Drops the email without sending a notification to the sender.

#### Notify Sender

Select to notify the sender that the email contains sensitive information.



**Figure 396: Data Protection**

#### Related tasks

[Add SPX Templates](#) on page 446

[Add a Data Control List](#) on page 441

#### Add POP-IMAP Scan Policy

**This feature requires a subscription. It can be configured but cannot be enforced without a valid Email Protection subscription.**

Add a POP-IMAP scan policy to detect incoming and outgoing spam in POP/S and IMAP/S traffic.

1. Go to **Protect > Email > Policies** and click **Add Policy**. Click **POP-IMAP Scan**.
2. Enter a **Name** for the policy.
3. Enter email address or domain group details.

#### Sender

To specify the sender email addresses, select from the following options:

Contains: Specify the keywords to be matched with the senders' email addresses. Example: If you specify the keyword mail, the rule applies to senders' email addresses such as example@examplemail.com, sophosmail@example.com.

Equals: Specify the senders' exact email addresses.

To add a list of keywords or email addresses, click **Create New**.

#### Recipient

To specify the recipient email addresses select from the following options:

Contains: Specify the keywords to be matched with the recipient email addresses. Example: If you specify the mail, the rule applies to recipient email addresses such as example@examplemail.com, sophosmail@example.com.

Equals: Specify the recipients' exact email addresses.

To add a list of keywords or email addresses, click **Create New**.

Sender *	Contains	Any
Recipient *	Contains	Any

**Figure 397: Email Address/Domain Group**

4. Select from the following **Filter Criteria** based on which the specified action is to be taken:

#### Inbound Email is

Select from the following options:

Spam Probable Spam Virus Outbreak Probable Virus Outbreak

#### Source IP/Network Address

Sender's IP address matches the specified IP address.

#### Message Size

Sender's email size matches the specified restriction of message size.

#### Message Header

Select from the following message headers to match the specified keyword:

Subject From To Other

Select the type of keyword match from the following options:

Contains: Specify the keywords to be matched with the message header.

Equals: Specify the exact match to the actual headers.

### **None**

Select to create a policy between specific senders and recipients without imposing any other condition.

**Figure 398: Filter Criteria**

5. Select the action.

#### **Action**

Action to be taken from the following options:

##### **Available Options:**

Accept: Email is accepted and delivered to the intended recipient. Prefix Subject: Email is accepted and delivered to the intended recipient after adding a prefix to the subject line. Specify the prefix in the **To** field. You can set the prefix to indicate the filter criteria.

Example:

Original subject line: Test mail

Tagged content: Probable Spam

Recipient receives email with the subject line: ‘Probable Spam: Test mail’

6. Click Save.

#### **Data Control List**

**This feature requires a subscription. It can be configured but cannot be enforced without a valid Email Protection subscription.**

**This feature is available in Cyberoam Models CR15iNG and above, and all Sophos UTM and Sophos Firewall Models.**

You can create a Data Control List of confidential data by selecting from the Content Control List (CCL). The device provides CCLs based on expert definitions for common financial and personally identifiable data types (example: credit card and social security numbers, postal and email addresses).

Subsequently, you can use Data Control Lists to set Data Protection for emails.

#### **Add a Data Control List**

**This feature requires a subscription. It can be configured but cannot be enforced without a valid Email Protection subscription.**

**This feature is available in Cyberoam Models CR15iNG and above, and all Sophos UTM Models.**

**Add Data Control List** allows you to create a list of confidential data types. The device provides Content Control Lists (CCL) based on expert definitions for common financial and personally identifiable data types.

1. Go to **Protect > Email > Data Control List** and click **Add**.
2. Enter the name.
3. Select the CCLs (Content Control List) from the list. Filter the CCLs based on **Type** and **Region**.

Name *	<input type="text"/>
CCLs *	<div style="display: flex; justify-content: space-between;"> <span>Type <input type="button" value="All"/></span> <span>Region <input type="button" value="All"/></span> </div> <p><input checked="" type="checkbox"/> Show only selected</p> <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Postal addresses [Global]           <ul style="list-style-type: none"> <li><input type="checkbox"/> Postal addresses [Australia]</li> <li><input type="checkbox"/> Postal addresses [Canada]</li> <li><input type="checkbox"/> Postal addresses [Germany]</li> <li><input type="checkbox"/> Postal addresses [Spain]</li> <li><input type="checkbox"/> Postal addresses [France]</li> <li><input type="checkbox"/> Postal addresses [Hong Kong]</li> <li><input type="checkbox"/> Postal addresses [Ireland]</li> <li><input type="checkbox"/> Postal addresses [Italy]</li> <li><input type="checkbox"/> Postal addresses [UK]</li> </ul> </li> </ul>

**Figure 399: Data Control List**

4. Click **Save**.

#### Related tasks

[Add SMTP Route and Scan Policy](#) on page 435

#### SMTP Quarantine

SMTP Quarantine is available only in Sophos Firewall XG105, Cyberoam CR25iNG, Sophos UTM SG105, and higher models.

This feature requires a subscription. It can be configured but cannot be enforced without a valid Email Protection subscription.

The **SMTP Quarantine** allows you to filter the quarantined emails. The page displays all the emails quarantined by the device if they are found to be:

- From a blocked Source IP Address
- Destined to a blocked Destination IP Address
- Virus-infected
- Oversized
- Containing a Blocked Header
- Containing unscannable content or a protected attachment
- blocked by an RBL
- blocked by a Data Protection (DP)
- Spam
- Found malicious by Sandstorm
- quarantined due to any other reason

Use the filter to search for mails from the list of quarantined emails.

The filter result displays a list of all the quarantined emails based on the filter criteria.

**Total utilization** displays the percentage of the quarantine area used by quarantined emails. Once the quarantine repository is full older emails are purged.

### Quarantine Digest

The Quarantine Digest is an email containing a list of quarantined emails filtered by the device and held in the user's quarantine area. If configured, the user receives a Quarantine Digest as per the frequency set in **Email > Quarantine Digest**. The digest also provides a link to the User Portal from where the user can access quarantined emails and take the required action.

### Releasing Quarantined Email

Either the Administrator or the user can release the quarantined Emails. Administrator can release the quarantined Emails from the Quarantine Area while the user can release them from his User Portal. Released quarantined Emails are delivered to the intended recipient's inbox. The Administrator can access the Quarantine Area from **Email > SMTP Quarantine**, while user can log on to the User Portal and access the Quarantine Area from **SMTP Quarantine**. If Quarantine Digest is configured, user will receive Digest of the quarantined mails as per the configured frequency.



#### Note:

- Virus-infected emails and the emails found malicious by Sandstorm cannot be released.
- To delete Sandstorm related emails, you need Read-Write permission for Sandstorm Activity.

**Figure 400: SMTP Quarantine**

### Mail Spool

**Mail Spool appears only when MTA (Mail Transfer Agent) mode is enabled. MTA mode is available only in Sophos Firewall XG105, Cyberoam CR25iNG, Sophos UTM SG105, and higher models.**

**This feature requires a subscription. It can be configured but cannot be enforced without a valid Email Protection subscription.**

**Mail Spool** displays emails that are waiting to be delivered. You can delete or retry sending these emails. This page does not display discarded emails.

1. Specify the filter criteria.
2. You can delete or retry sending the filtered emails.



#### Note:

- To delete or retry sending Sandstorm-related emails, you need Read-Write permission for Sandstorm Activity.
- The device retries sending emails for three days. At the end of an additional four days, it discards the emails. You can view the discarded emails from **Mail Logs**.

### Mail Logs

**Mail Logs** appears only when MTA (Mail Transfer Agent) mode is enabled. MTA mode is available only in Sophos Firewall XG105, Cyberoam CR25iNG, Sophos UTM SG105, and higher models.

This feature requires a subscription. It can be configured but cannot be enforced without a valid Email Protection subscription.

**Mail Logs** allows you to view and filter email logs.

1. Specify the filter criteria.
2. Specify the criteria for **Result Filter** to display logs based on delivery status.
3. Specify the criteria for **Reason Filter** to display logs based on the scan result.
4. Click **Filter**.

The screenshot displays a user interface for filtering mail logs. It includes fields for 'Start Date' (2016-12-16) and 'End Date' (2016-12-16). A dropdown for 'Recipient Domain' is set to 'All'. The 'Result Filter' section contains six checked checkboxes: Delivered, Rejected, Bounced, Dropped, Quarantined, and Deleted. The 'Reason Filter' section contains nine checked checkboxes: Malware, Spam, File Filter, Unscannable, Data Protection, SPX Encryption, SPX Failure, RBL, and Sandstorm. Below these sections are 'Filter' and 'Clear' buttons.

**Figure 401: Mail Logs**

## Encryption

SPX Encryption is available in Sophos Firewall XG105 and higher models, Cyberoam CR25iNG and higher models, and all Sophos UTM Models.

This feature requires a subscription. It can be configured but cannot be enforced without a valid Email Protection subscription.

### What is SPX Encryption?

SPX (Secure PDF Exchange) encryption is a next-generation version of email encryption. It is clientless and extremely easy to set up and customize in any environment. Using SPX encryption, email messages and any attachments sent to the Device are converted to a PDF document, which is then encrypted with a password. You can configure the Device to allow senders to select passwords for the recipients, or the server can generate the password for the recipient and store it for that recipient, or the server can generate one-time passwords for recipients.

When SPX encryption is enabled, there are two ways in which emails can be SPX encrypted:

- The user can download the Sophos Outlook Add-in from **User Portal**. After having it installed, an Encrypt button is displayed in the Microsoft Outlook user interface. To encrypt a single message, the user needs to click the Encrypt button and then write and send the message.

#### Note:

If you do not use Outlook you can also trigger SPX encryption by setting the header field X-Sophos-SPX-Encrypt to "yes".

- In the Data Protection feature, you can enforce SPX encryption of Emails containing sensitive data (see **Email > Policies > SMTP Policy**).

The encrypted message is then sent to the recipient's mail server. Using any PDF reader, the recipient can decrypt the message with the password that was used to encrypt the PDF. SPX-encrypted email messages are accessible on all popular smartphone platforms that have native or third-party PDF file support, including Android, iOS, BlackBerry and Windows Mobile devices.

The SPX-encrypted email contains a **Reply** button which links to the SPX Reply Portal. Using the SPX Reply Portal, the recipient is able to answer to the email in a secure way.

## SPX Configuration

### Default SPX Template

Select the SPX Template to be used by default. The Default Template is used if any user explicitly SPX-encrypts an email and no template is selected in the Content Scanning Rule.

The user can SPX-encrypt an Email by:

- Manually setting the Email header **X-Sophos-SPX-Encrypt** to "yes".
- Installing the Sophos Outlook Add-on and clicking **Encrypt** before sending the Email.

If the Default SPX Template is set to **None**, then SPX encryption is not applied to Email.

### Allow Secure Reply for

Enter the maximum time (in days) in which recipient can securely reply to an SPX-encrypted email using the SPX Reply Portal.

### Keep Unused Password for

Enter the expiry time in days of an unused password.

For example, if Keep Unused Password for is set to 3 days, the password will expire at 0 o'clock 3 days after being generated if no SPX encrypted message has been sent for a specific recipient.

Default: 30 days

### Allow Password Registration for

Enter the time in days after which the link to Password Registration Portal expires.

Default: 10 days

### Send Error Notification To

Specify whom to send a notification when an SPX error occurs. You can send the notification to the sender or you can send no notification at all. Error messages will always be listed in the SMTP log.

Default SPX Template	<input type="button" value="Default Template"/>
Allow Secure Reply for	30 <input type="button" value="Day(s)"/>
Keep Unused Password for	30 <input type="button" value="Day(s)"/>
Allow Password Registration for	10 <input type="button" value="Day(s)"/>
Send Error Notification to	<input type="button" value="Sender Only"/> 

**Figure 402: SPX Configuration**

## SPX Portal Settings

### Host Name

Enter the IP Address or Domain on which the Password Registration Portal is hosted.

#### Allowed Network(s)

Enter the networks from which password registration requests will be accepted.

#### Port

Enter the port on which the SPX Password Registration Portal should listen.

Default: 8094

Hostname	<input type="text" value="None"/>
Allowed Network(s)	<input type="text" value="Any"/> <span style="color: red;">-</span>
<a href="#">Add New Item</a>	
Port	<input type="text" value="8094"/>

**Figure 403: SPX Portal Settings**

#### SPX Password Reset

##### Reset Password for

Enter the Email Address for the recipient for whom you want to reset the password. New SPX email to this address requires the recipient to obtain a new password from the sender.

Reset Password for	<input type="text" value="Enter Email Address"/>	<a href="#">Reset</a>
--------------------	--------------------------------------------------	-----------------------

**Figure 404: Password Reset**

#### SPX Templates

The SPX template defines the layout of the PDF file, password settings and recipient instructions. You can also define different SPX templates. So, if you are managing various customer domains, you can assign them customized SPX templates containing, for example, different company logos and texts.

Name	Password Type	
<input type="checkbox"/> Default Template	Specified by sender	<a href="#">Edit</a>

**Figure 405: SPX Templates**

#### Add SPX Templates

**SPX Encryption is available in Sophos Firewall XG105 and higher models, Cyberoam CR25iNG and higher models, and all Sophos UTM Models.**

**This feature requires a subscription. It can be configured but cannot be enforced without a valid Email Protection subscription.**

This page allows you to define new SPX Templates or modify existing templates.

1. Go to **Protect > Email > Encryption > SPX Templates** and click **Add**.
2. Enter parameter values for the following basic settings.

#### Name

Specify the name to uniquely identify the template. The name should be a string containing alphanumeric and special characters EXCEPT forward slash (/), backslash (\), comma (,), double quote ("") and single quote (').

#### Description

Specify details of the template.

#### Organization Name

Specify the organization name to be displayed on notifications concerning SPX sent to the administrator or the email sender, depending on your settings.

#### PDF Encryption

Select the encryption standard of the PDF file.

#### Page Size

Select the page size of the PDF file.

Name *	<input type="text"/>
Description	<input type="text"/>
Organization Name	<input type="text"/>
PDF Encryption	AES / 128
Page Size	A4

**Figure 406: General Settings**

3. Enter Password Settings.

#### Password Type

Select how you want to generate the password for accessing the encrypted email message. The sender always has to take care of transferring the password in a safe way to the recipient, unless you select **Specified by recipient**.

#### Available Options:

##### Specified by Sender:

If you select this, the email sender should provide the password. The sender has to enter the password into the Subject field, using the following format:  
`[secure:<password>]<subject text>` where <password> is the password to open the encrypted PDF file and <subject text> is the random subject. Of course, the password will be removed by the Device before the email is sent to the recipient.

##### Generated one-time password for every email:

The Device automatically creates a new password for each affected email. An email notification is mailed to the sender containing instructions and the one-time generated password.

The HTML content of this Email can be customized from **Notification Subject** and **Notification Body**. You can reset to the default content by clicking **Reset**.

#### **Generated and stored for recipient:**

The Device automatically creates a recipient-specific password when the first email is sent to a recipient. This password will be sent to the sender. With the next email, the same password is used automatically. The password will expire when it is not used for a configured time period, and it can be reset by the administrator, see [Encryption](#).

The HTML content of this Email can be customized from **Notification Subject** and **Notification Body**. You can reset to the default content by clicking **Reset**.

#### **Specified by recipient:**

If you select this, the email recipient should provide the password. The recipient receives an email notification containing a link leading to the Password Registration Portal to register a password and the Sender receives a failure notification. After registration, the recipient is able to view the current encrypted mail and any future encrypted mails using the same password from this or other senders from the same organization.



**Note:** The Recipient's password generated via **Specified by recipient** method and **Generated and stored for recipient** are mutually exclusive. The recipient will have to use the respective password when email is received after SPX Encryption using different methods.

A screenshot of a user interface showing a dropdown menu labeled "Password Type \*". The menu is open and displays two options: "Specified by sender" (which is highlighted) and "Generated and stored for recipient".

**Figure 407: Password Settings**

#### 4. Specify Recipient Instructions:

##### **Instructions for Recipient**

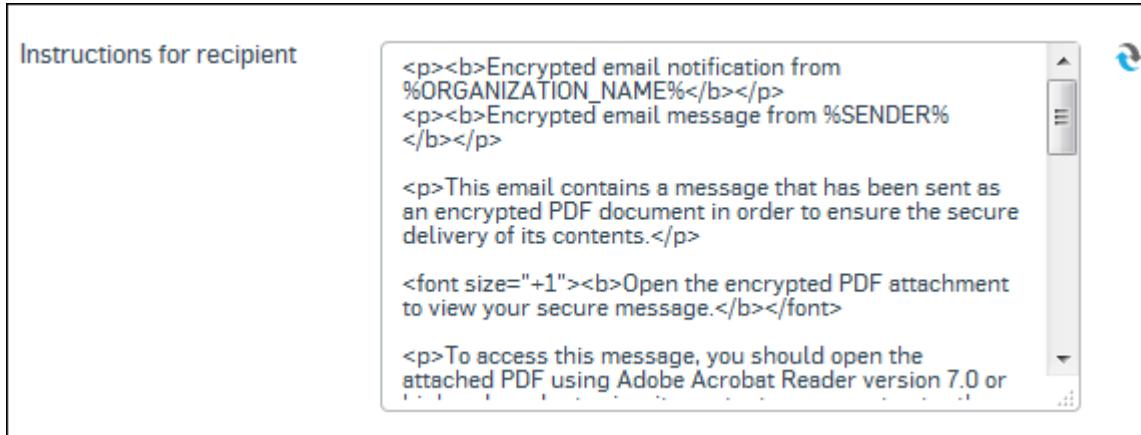
The body of the email that is sent from the Device to the email recipient containing instructions concerning the encrypted email. Simple HTML markup and hyperlinks are allowed. You can also use variables, e.g.,

%%ORGANIZATION\_NAME%%



**Tip:** The Default SPX Template on this tab contains all available variables and gives a useful example of recipient instructions. The variables used are:

- ENVELOPE\_TO: The recipient for whom the password is generated.
- PASSWORD: The password to open SPX encrypted Email
- ORGANIZATION\_NAME: The name provided in the **Organization Name** field.
- SENDER: The sender of the email.
- REG\_LINK: The link to the Registration Portal for registering the password.

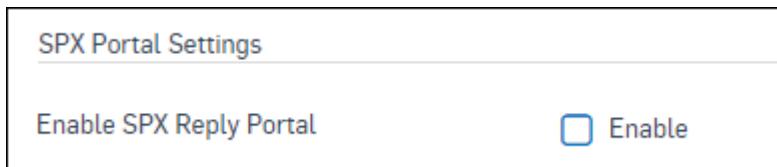


**Figure 408: Recipient Instructions**

## 5. Enable SPX Portal Settings

### Enable SPX Reply Portal

Click to enable users to securely reply to SPX-encrypted emails using the SPX Reply Portal. You also have the option to **Include Original Body into Reply**.



**Figure 409: SPX Portal Settings**

### Related tasks

[Add SMTP Route and Scan Policy](#) on page 435

## General Settings

This feature requires a subscription. It can be configured but cannot be enforced without a valid Email Protection subscription.

Email Configuration allows you to configure the general settings Email traffic. This page contains the following sections.

### SMTP Deployment Mode

**MTA mode is available only in Sophos Firewall XG105, Cyberoam CR25iNG, Sophos UTM SG105, and higher models.**

Click button to switch to MTA/Legacy Mode.

In MTA Mode, Device acts as a Mail Transfer Agent (MTA). In Legacy Mode, Device acts as a transparent proxy.

When acting as an MTA, Device is responsible for routing Emails to and from the protected Email Server(s). In this state Device allows you to:

- configure relay of inbound and outbound Emails from **Email > Relay Settings**.
- set up multiple SMTP Profiles to protect multiple Domains on your internal Email Server or multiple Email Servers from **Email > Policies > SMTP Policies**.
- view email messages that are either waiting for delivery or have produced an error in the **Email > Mail Spool**.
- view the logs for all the emails processed by the Device from **Email > Mail Logs**.

Default: MTA Mode is enabled.

**Note:**

- On enabling MTA Mode, a firewall rule to allow SMTP/SMTPTS traffic is automatically created.
- If you have migrated from CyberoamOS to SFOSv16 OR SFOSv15 to SFOSv16, Legacy Mode will be enabled by default.

Device acts as a Transparent Proxy.

You can switch to MTA Mode wherein Device acts as a Mail Transfer Agent (MTA).

[Switch to MTA Mode](#)

**Figure 410: SMTP Deployment Mode**

## Banner Settings

### Append Banner to All Outbound Messages

Enable to add a banner at the end of all outgoing Email messages.

The banner is appended ONLY when SMTP and SMTPTS Scanning is enabled in the relevant Business Application Policy(s).

### Email Banner

Specify a banner to be added to all outgoing Emails. Only text banners are allowed.

Example:

*This email contains confidential information. You are not authorized to copy the contents without the consent of the sender. Please do not print this email unless it is absolutely necessary. Spread environmental awareness.*



**Figure 411: Banner Settings**

## SMTP Settings

### SMTP Hostname

Specify the SMTP hostname to be used in HELO and SMTP banner strings. By default, Device uses 'Sophos' as hostname.

**Note:** For Legacy Mode, this hostname is applicable only to system-generated notification emails.

### Don't Scan Emails Greater Than

Specify maximum file size (in KB) for scanning. Files exceeding this size received through SMTP/S will not be scanned.

Default - 1024 KB

Specify 0 to increase the default file size scanning restriction to 51200 KB.

#### Action for Oversize Email

Specify the action for Oversize Emails.

#### Available Options

Accept: All the oversize mails are forwarded to the recipient without scanning. Reject: All the oversize mails are rejected and sender is notified. Drop: All the oversized mails are dropped, without notifying the sender.

#### Bypass Spam Check for SMTP/S Authenticated Connections (Available in Legacy Mode only)

Enable to bypass Spam Scanning for Email messages received over SMTP/S connections authenticated by the Email Server.

#### Verify Sender's IP Reputation

Click to verify the reputation of the sender IP Address. When enabled, the Device dynamically checks the sender's IP Address of all Emails. If the IP Address is found to be responsible for sending spam email or malicious contents, the Device takes action as per the configured Scanning Rules.

If enabled, specify an action for Confirmed Spam Emails and Probable Spam Emails.

#### Available Options

Accept: All the spam Emails are forwarded to the recipient after scanning as per the configuration. Reject: All the spam mails are rejected and a notification is sent to the Email sender. Drop: All the spam mails are dropped, without notifying the sender.

As it is a global option, if spam scanning is enabled, all the mails will first be subjected to IP Reputation filtering followed by filtering based on actions configured in the spam policy.

Default - Disable

#### SMTP DoS Settings

Enable to configure SMTP DoS Settings which protect the network from SMTP DoS Attacks.

If this is enabled, specify values for Maximum Connections, Maximum Connections/Host, Maximum Emails/Connection, Maximum Recipients/Email, Email Rate per Minute/Host and Connections Rate per Second/Host.

#### Maximum Connections (Available if SMTP DoS Settings Enabled)

Specify maximum number of connections that can be established with the Email Server.

Default - 1024

Acceptable Range - 1 - 20000

#### Maximum Connections/Host (Available if SMTP DoS Settings Enabled)

Specify maximum number of connections allowed to the Email Server from a particular host.

Default - 64

Acceptable Range - 1 - 10000

#### Maximum Emails/Connection (Available if SMTP DoS Settings Enabled)

Specify maximum number of Emails that can be sent in a single connection.

Default - 512

Acceptable Range - 1 - 1000

#### Maximum Recipients/Email (Available if SMTP DoS Settings Enabled)

Specify maximum number of recipients for a single Email.

Default - 100

Acceptable Range - 1 - 256

#### Email Rate per Minute/Host (Available if SMTP DoS Settings Enabled)

Specify number of Emails to be sent from a particular host in one minute.

Default - 512

Acceptable Range - 1 - 20000

#### Connection Rate per Second/Host (Available if SMTP DoS Settings Enabled)

Specify number of connections allowed to the Email Server from a particular host in one second.

Default - 8

Acceptable Range - 1 - 20000

SMTP Hostname	Sophos	This will be used in HELO string for system-generated notification emails.
Don't Scan Emails Greater Than *	0 KB	Enter 0 for default size restriction of 51200 KB
Action for Oversize Emails *	<input checked="" type="radio"/> Accept <input type="radio"/> Reject <input type="radio"/> Drop	
Bypass Spam Check For SMTP/S Authenticated Connections	<input type="checkbox"/>	
Verify Sender's IP Reputation	<input checked="" type="checkbox"/> Enable	
Confirm Spam Action	Reject	
Probable Spam action	Reject	
SMTP DoS Settings	<input checked="" type="checkbox"/> Enable	
Maximum Connections *	5000	
Maximum Connections/Host *	100	
Maximum Emails/Connection *	1000	
Maximum Recipients/Email *	100	
Emails Rate *	1000	Per Minute/Host
Connections Rate *	100	Per Second/Host

**Figure 412: SMTP Settings**

#### POP/S and IMAP/S Settings

##### Don't Scan Emails Greater Than

Specify maximum file size (in KB) for scanning. Files exceeding this size received through POP/IMAP will not be scanned.

Default - 1024 KB

Specify 0 to increase the default file size restriction to 10240 KB.

##### Recipient Headers

Specify Header value to detect recipient for POP3/IMAP.

Default - Delivered-To, Received, X-RCPT-TO

Don't Scan Emails Greater Than \* 1024 KB Enter 0 for default size restriction of 10240 KB

Recipient Headers

Headers	Add (+)
Delivered-To	-
Received	-
X-RCPT-TO	-

**Figure 413: POP/S and IMAP/S Settings**

## SMTP TLS Configuration

### TLS Certificate

Select the CA Certificate or Server Certificate for scanning SMTP traffic over SSL from the available options.

### Available Options

Default Appliance Certificate Security Appliance\_SSL\_CA List of custom CA Certificates and Server Certificates, if added. You can create the custom CA Certificate from **Certificates > Certificate Authorities** and custom Server Certificate from **Certificates > Certificates**.

### Allow Invalid Certificate

If enabled, SMTP over SSL connections will be allowed with an invalid certificate from the Email Server. Disable this option to reject such connections.

Default - Enable

### Require TLS Negotiation with Host/Net

Select the remote host (Email Server) or network from available options on whose connections TLS encryption is to be enforced. In other words, the Device will always initiate TLS-secured connections when Emails are to be sent to selected hosts/networks. If TLS is enforced but connection cannot be established, then Emails to that remote host/network are discarded.

### Require TLS Negotiation with Sender Domain

Specify the Sender Domain(s) on whose Email connections TLS encryption is to be enforced.

Sender Domain is the domain of the Email sender. Emails from the specified Sender Domain will be sent over TLS-encrypted connections only. If TLS is enforced but connection cannot be established, then Emails from that sender domain are discarded.

### Skip TLS Negotiation Hosts/Nets

Select the remote host (Email Server) or network from available options on whose connections TLS encryption is to be skipped or bypassed. When configured, SMTP connections to selected hosts will be established in clear text and unencrypted.

TLS Certificate *	<input type="text" value="SecurityAppliance_SSL_CA"/> <input type="button" value="▼"/>
Allow Invalid Certificate	<input checked="" type="checkbox"/> Enable
Require TLS Negotiation with Host/Net	<input type="button" value="Add New Item"/>
Require TLS Negotiation with Sender Domain	<input type="button" value="Add New Item"/>
Skip TLS Negotiation Hosts/Nets	<input type="button" value="Add New Item"/>

**Figure 414: SMTP TLS Configuration**

### POP and IMAP TLS Configuration

#### TLS Certificate

Select the CA for scanning POP and IMAP traffic over SSL from the available options.

#### Available Options

DefaultSecurityAppliance\_SSL\_CAList of custom CAs if added. You can create the custom CA from **Certificates > Certificate Authorities**.

#### Allow Invalid Certificate

If enabled, POP and IMAP over SSL connections will be allowed with invalid certificate from the Mail Server. Disable to reject such connections.

Default - Enable

TLS Certificate *	<input type="text" value="SecurityAppliance_SSL_CA"/> <input type="button" value="▼"/>
Allow Invalid Certificate	<input checked="" type="checkbox"/> Enable

**Figure 415: POP and IMAP TLS Configuration**

### Email Journaling (Available in Legacy Mode only)

Email being one of the most important communication and business tools in use by organizations, email journaling has become an integral part of every organization.

Using the Device's Email Journaling, the administrator can store all incoming Emails, or Emails for a specific recipient or a group of recipients and thereby keep a close watch over data leakage.

The device can journal all Emails intended for single or multiple recipients and can forward them to a single administrator or multiple administrators.

This section displays a list of the archivers created and provides options to [add a new archiver](#), [update the parameters of existing archiver](#), or delete the archiver. You can filter the list based on recipient name.

<input type="checkbox"/> Name	Recipient	Send Copy To	Manage
No Records Found			

**Figure 416: Email Journaling**

### Spam Check Exceptions

To bypass spam scanning of certain domains, define the domains as Spam Check Exceptions. The page lists all the domains configured to be exempted from spam scanning.

It also provides the options to add a new domain and delete an existing domain.

Domain Name \*

**Add**

<input type="checkbox"/> Domain Name	Manage	Delete
No Records Found		

**Figure 417: Spam Check Exceptions**

### Malware Protection

**Malware Protection is available in Sophos Firewall XG105, Cyberoam CR500iNG, Sophos UTM SG105, and higher models.**

Sophos Firewall offers dual anti-virus scanning, wherein traffic is scanned by two (2) anti-virus engines. Traffic is first scanned by the primary engine, and then by the secondary engine.

#### Primary Anti Virus Engine

Select the primary anti-virus engine for traffic scanning. For dual scan, packets are first scanned by the primary engine and then by the secondary engine. For single scan, only the primary engine is used.

#### Available Options

SophosAvira

**Note:** Selecting **Avira** will disable Sandstorm in all SMTP Policies with Single Anti-Virus Scanning.

Primary Anti-Virus Engine

Sophos

**Apply**

**Figure 418: Malware Protection**

## Smarthost Settings

A smarthost is a Mail Transfer Agent (MTA) which acts as an intermediate server between the sender's and recipient's email servers. On configuring a smarthost, the device redirects outbound emails to the designated server, which are then routed to the recipient's email server.

Enable **Use Smarthost**.

### Hostname

Select the host that will act as a smarthost.



**Note:** You cannot configure Smarthost as the device's interface IP address. It will result in a routing loop.

### Port

Enter the port.

Default: 25

### Authenticate Device with Smarthost

Select if the smarthost requires the device to authenticate before routing emails. Both Plain and Login authentication types are supported. Enter a **Username** and **Password**.

The screenshot shows the 'Smarthost Settings' configuration page. At the top left is a title bar with the page name. Below it is a section with a checked checkbox labeled 'Use Smarthost' and an information icon. To the right are two input fields: 'Hostname' (empty) and 'Port' (set to 25). Below these are two more sections: 'Authenticate Device with Smarthost' (checked) and 'Username' (empty) and 'Password' (represented by a series of dots). A 'Change Password' link is located next to the password field. At the bottom is a large blue 'Apply' button.

**Figure 419: Smarthost Settings**

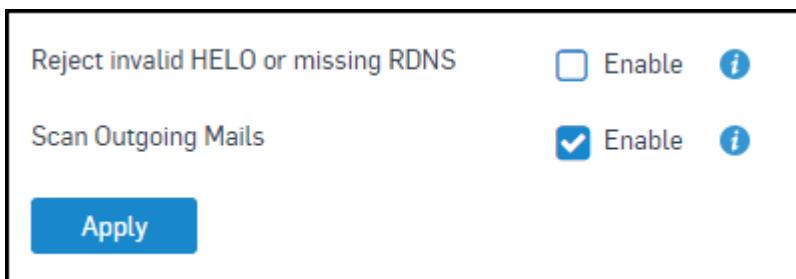
### Advanced SMTP Settings (Available in MTA Mode only)

#### Reject invalid HELO or missing RDNS

Select this option if you want to reject hosts that send invalid HELO/EHLO arguments or lack RDNS entries. Select **Do strict RDNS checks** if you want to additionally reject email from hosts with invalid RDNS records. An RDNS record is invalid if the found hostname does not resolve back to the original IP address.

### Scan Outgoing Mails

Enable to scan all outgoing email traffic. Email is quarantined if found to be malware infected, or marked as Spam.



**Figure 420: Advanced SMTP Settings**

### Address Groups

Policies are applied on Email Addresses. To make configuration easier and simpler, the Administrator can group the addresses that require the same scanning policy. The policy applied to the address group is applicable to all the group members. Hence when the group is used in a number of rules, it becomes much easier to add or remove addresses from the group rather than updating individual rules. Hence, just with the one update, the Administrator can re-align the rules.

An Address Group is a grouping by:

- Email Address or Domain
- IP Address
- RBL (Real time black hole List) (applicable only for the spam email)

An address can be a member of multiple groups.

An RBL is a list of IP Addresses whose owners are responsible for spam or are hijacked for a spam relay. These IP Addresses might also be used for spreading viruses. The Device checks each RBL for the connecting IP Address and the action configured in the policy is taken if the IP Address is found in any of the RBL lists. The Administrator can directly use the two default RBL groups shipped with the Device or update them as per their requirement:

- Premium RBL Services
- Standard RBL Services

The Address Group page displays a list of all the default and custom groups and provides options to add a new group, update the parameters, import addresses in the existing group, or delete the group. You can sort the list based on address group name.

### Add Address Group

1. Go to **Protect > Email > Address Group** and click **Add**.
2. Enter a name and description.
3. **Group Type:** Select to add email addresses or domains to the address group.

#### Available Options:

##### RBL (IPv4) or RBL(IPv6):

Select to add RBLs of IPv4 or IPv6 addresses or domain names.

If the connecting IP address is found on the RBL, the device takes the action specified by the relevant policy.

##### Email Address/Domain:

Select to add the email address or domain name.

**Import:** Select to upload a CSV or text file.

**Manual:** Select to add individual email addresses or domains.

**Note:**

- You can import a maximum of 400 email addresses or domains in a single file.
- Invalid and duplicate entries are not imported.

The screenshot shows a configuration interface for an 'Address Group'. The fields include:

- Name \***: An input field labeled 'Enter Name'.
- Description**: An input field labeled 'Enter Description'.
- Group Type**: Radio buttons for 'RBL (IPv4)', 'RBL(IPv6)', and 'Email Address/Domain'. 'Email Address/Domain' is selected.
- Type**: Radio buttons for 'Import' and 'Manual'. 'Import' is selected.
- Email Address(es)/Domain(s) \***: An input field.
- Search / Add**: A button with a magnifying glass icon.

**Figure 421: Address Group**

4. Click Save.

**Relay Settings**

**Relay Settings** appears only when MTA (Mail Transfer Agent) mode is enabled. MTA mode is available only in Sophos Firewall XG105, Cyberoam CR25iNG, Sophos UTM SG105, and higher models.

This feature requires a subscription. It can be configured but cannot be enforced without a valid Email Protection subscription.

You can configure an SF Device to act as an email relay, allowing mail servers to send emails through it. You can specify the criteria for one or all parameters.

1. Specify the criteria for **Host Based Relay** to allow or block the specified hosts/networks from using the device as email relay.
  - a) Select **Allow Relay from Hosts/Networks** to allow the specified hosts or networks.
 

**Note:** Do not select **Any**. This causes the device to act as an open relay server, allowing anyone on the Internet, including spammers to send messages through the device.
  - b) Select **Block Relay from Hosts/Networks** to block the specified hosts or networks.
2. Specify the criteria for **Upstream Host** to select the upstream hosts/networks from which the device allows or blocks inbound emails.
  - a) To set **Allow Relay from Hosts/Networks**, select from the list. If all of your inbound emails are routed via an upstream filtering service or ISP, enter their IP addresses here. Select **Any** to accept emails directly from the sender.
  - b) To set **Block Relay from Hosts/Networks**, select from the list.

**Note:**

- For **Allow Relay from Hosts/Networks**, only emails that are destined to an internal domain are accepted.
- The device allows hosts/networks specified in the **Allow** list even when they are part of the **Block** list. This can happen when you select a group or network that they belong to, or 'Any' in the **Block** list.

3. Specify the **Authenticated Relay Settings** to allow only authenticated users and groups to use the device as email relay.
  - a) Select **Enable Authenticated Relay**.
  - b) Select the **Users or Groups** from the list.
4. Click **Apply**.

### File Types

A file type is a classification that is determined by file extension and MIME header. You can include file types in web policies to control access to files that match the specified criteria. The default file types contain some common criteria and you can create additional types.

#### Using File Types with Policy Rules

You can create file types to control access to files on a more granular level. For example, you may want to allow access to SQL files but deny access to all other database files. In this case, you would create a file type for SQL files and a policy that specifies the following rules in the following order:

1. Allow access to SQL files
2. Block access to all database files

### Add File Type

1. Go to **Protect > Web > File Type** and click **Add**.
2. Type a name.
3. (Optional) Select a template.

You can select from predefined or custom file types. If you do not wish to use a template, choose **Blank**.

4. Specify the file extension and MIME header.

Name *	<input type="text" value="Name"/>
Description	<input type="text" value="Description"/>
Template	<input style="width: 100px; height: 20px; border: 1px solid #ccc; border-radius: 5px; padding: 2px 5px;" type="text" value="Blank"/> <span style="font-size: small;">▼</span>
File Extension *	<input style="width: 100%; height: 100px; border: 1px solid #ccc; border-radius: 5px; padding: 2px; font-size: small;" type="text" value="Add Extensions here"/> <small>Use comma as a separator to enter multiple entries.</small>
MIME Header *	<input style="width: 100%; height: 100px; border: 1px solid #ccc; border-radius: 5px; padding: 2px; font-size: small;" type="text" value="Add MIME Headers here"/> <small>Use comma as a separator to enter multiple entries.</small>

**Figure 422: Add File Type**

### Quarantine Digest

**Quarantine Digest** is available only in Sophos Firewall XG105, Cyberoam CR25iNG, Sophos UTM SG105, and higher models.

This feature requires a subscription. It can be configured but cannot be enforced without a valid Email Protection subscription.

**Quarantine Digest** allows you to set the frequency at which the digest email is sent to the user. You can enable or disable user access to quarantined emails on the user portal. You can also enable quarantine digest for all users or to specific users and groups.

Quarantine Digest provides the date and time of message receipt, sender and recipient's email addresses and subject of the message.

### Quarantine Digest Settings for All Users

1. Go to **Protect > Email > Quarantine Digest**.
2. Select **Enable Quarantine Digest** to email the digest to all users.
  - a. Set the **Email Frequency** of the digest. Set the interval, time, and day of week, based on the selection.
  - b. In the **From Email Address** box, enter the address from which the email is to be sent.
  - c. In the **Display Name** box, specify the name of the quarantine digest sender.
  - d. Click **Send Test Email**. Enter the **To Email Address** and click **Send**.
  - e. To set the IP address of the user portal, select the **Reference User Portal IP** from the list.

 **Note:** Users located behind the selected port can click the "My Account" link in the digest email to gain access to quarantined emails on the user portal. Others can access the user portal by typing `https://<IP Address of SF Device>` in the browser.

Example: If Port1 is selected as the **Reference User Portal IP**, only users located behind Port1 will be redirected to the user portal when they click on "My Account".

3. Click **Apply**.

### Override Quarantine Digest Settings for Specific Users

1. Go to **Protect > Email > Quarantine Digest**.
2. Click **Change User's Quarantine Digest Settings**, to apply the settings to specific users or groups.
3. Select the users or groups.
4. Click **Apply**.

The screenshot shows the 'Quarantine Digest' configuration page. At the top left is a checked checkbox labeled 'Enable Quarantine Digest'. Below it is a section for 'Email Frequency' with three radio buttons: 'Hourly' (unchecked), 'Daily' (checked), and 'Weekly' (unchecked). Underneath is a 'Send Email Daily At' field containing '10' in the hour dropdown and '00' in the minute dropdown. To the right of this field is a note about users behind selected ports. Below the frequency section are fields for 'From Email Address' (containing 'admin@sophos.com') and 'Display Name' (containing 'Quarantine Digest'). A large blue button labeled 'Send Test Email' is positioned below these. At the bottom is a field for 'Reference User Portal IP' with a dropdown menu showing 'PortA'.

**Figure 423: Quarantine Digest**

#### Related concepts

[Data Control List](#) on page 469

## Legacy Mode

### Policies

**This feature requires a subscription. It can be configured but cannot be enforced without a valid Email Protection subscription.**

This page allows configuration of SMTP Route and Scan Policies, SMTP Malware Scan Policies, SMTP Spam Scan Policies and POP-IMAP Scan Policies:

- SMTP Route and Scan Policies (MTA Mode)
- SMTP Malware Scan Policies (Legacy Mode)
- SMTP Spam Scan Policies (Legacy Mode)
- POP3-IMAP Scan Policies (MTA and Legacy Mode)

### SMTP Route and Scan Policies

**SMTP Route and Scan policies appear only when MTA (Mail Transfer Agent) mode is enabled. MTA mode is available only in Sophos Firewall XG105, Cyberoam CR25iNG, Sophos UTM SG105, and higher models.**

Device allows you to create SMTP Route and Scan policies which can be used to protect multiple Domains on your internal Email Server(s). Using these policies, device protects the server(s) from remote attacks and additionally provide powerful virus scanning, email encryption and email filtering services.

Click **Add Policy** and then **SMTP Route & Scan** to add a new policy. To update an existing policy, click the desired policy.

### SMTP Malware Scan Policies

**SMTP Malware Scan policies appear only when Legacy mode is enabled. The device acts as a transparent proxy.**

SMTP Malware Scan policies allow you to define action to be taken on emails if they are virus-infected or contain a protected attachment. Based on the action defined in rule, such emails can be delivered as they are, dropped, or cleaned and then delivered or quarantined.

A Malware Scan policy defines:

- whether to quarantine the email
- whether sender, receiver or administrator are to be notified
- whether to block the email containing a specified file type
- what action is to be taken if email is infected or contains a protected attachment: deliver as it is, drop, clean and then deliver



**Note:** You can also view the Quarantine from **Protect > Email > SMTP Quarantine** page.

A default SMTP Malware Scan policy named **default-smtp-av** is pre-configured in the device and applied to all SMTP traffic as soon as you subscribe to the Email Protection Module. We recommend that you create separate rules fine-tuned to your specific network requirements to minimize the possibility of threats.

Click **Add Policy** and then **SMTP Malware Scan** to add a new policy. To update an existing policy, click the desired policy.

### SMTP Spam Scan and POP-IMAP Scan Policies

**SMTP Spam Scan policies appear only when Legacy mode is enabled.**

**POP-IMAP Scan policy is available in both MTA and Legacy modes.**

When you subscribe to the Email Protection Module, SMTP Spam Scan and POP-IMAP Scan policies can be configured for particular senders and recipients.

A policy defines the action to be taken if an email is detected as Spam, Probable Spam, part of Virus Outbreak or Probable Virus Outbreak.

To reduce the risk of losing legitimate messages, the Spam Quarantine repository (a storage location) provides administrators with a way to automatically quarantine emails that are identified as spam. This helps in managing spam and probable spam quarantined mails so that the user can take appropriate actions on such emails.

A default POP-IMAP Scan policy named **default-pop-av** is pre-configured in the device and applied to all POP3/S and IMAP/S traffic so that whenever a virus gets detected in an email, the virus-affected attachment is stripped from the email and the email body is replaced with a notification message.

### **Detection of Spam attributes**

The device uses Content Filtering, and premium and standard Realtime Blackhole Lists (RBLs) to check for the spam attributes in SMTP/S, POP3/S and IMAP/S emails:

- Premium
- Standard

RBL is a list of IP Addresses whose owners refuse to stop the proliferation of spam, that is, owners who are responsible for spam or are hijacked for spam relay. The device checks each RBL for the connecting IP Address. If the IP Address matches one on the list, then the specified action in the policy is taken.

### **Add SMTP Malware Scan Policy**

**SMTP Malware Scan policies appear only when Legacy mode is enabled. The device acts as a transparent proxy.**

**This feature requires a subscription. It can be configured but cannot be enforced without a valid Email Protection subscription.**

The **Add SMTP Malware Scan Policy** page allows you to configure scan policy to detect malware in Email traffic and take appropriate action.

1. Go to **Email > Policies**, click **Add policy** and then click **SMTP Malware Scan**.
2. Enter a **Name** to identify the scan rule.
3. Enter **Email Address/Domain Group** details.

#### **Sender**

Select the sender name from the list of users.

Select **Any** if the rule is to be applied on all the senders.

You can also add RBLs or list of Email addresses by clicking **Create New link**.

#### **Recipient**

Select the recipient name from the list of users.

Select **Any** if the rule is to be applied on all the recipients.

You can also add RBLs or list of Email addresses by clicking **Create New link**.

<b>Email Address/Domain Group</b>	
<b>Sender *</b>	Any
<b>Recipient *</b>	Any

**Figure 424: Email Address/Domain Group**

4. Enter **Attachment Filter** details.

## Block File Types

Select file types to be blocked as an attachment to remove all the files that are a potential threat and to prevent virus attacks.

More than one file type can be selected using ctrl/shift keys.

Device contains a default list of File Types, with each Type containing relevant file extensions. Refer to **Email > File Type** to view the list of file extensions which can be blocked.

Select **All** to block Emails with any type of attachments.

Select **None** to allow Emails with any type of attachments.

## MIME Whitelist

If one or more File Type is selected in Block File Type, this field is populated with the corresponding MIME Headers that belong to selected File Type(s).

Select the MIME Header(s) of the selected File Type(s). Only selected headers are to be allowed while the rest in the selected File Type are to be blocked during Anti-virus scanning of Email attachments.



**Figure 425: Attachment Filter**

## 5. Specify Malware Filter details.

### Scanning

Select the scanning action.

#### Available Actions:

**Disable:** Emails are not scanned. **Enable:** Emails are scanned by the device's anti-virus engine.



#### Note:

In Sophos Firewall XG105, Cyberoam CR500iNG, and Sophos UTM SG105, and higher models, **Enable** is replaced by the following options.

**Single Anti-Virus:** The primary anti-virus engine scans the emails.

**Dual Anti-Virus:** The primary and secondary engines scan emails sequentially.

Select the **Primary Anti-Virus Engine** from **Protect > Email > General Settings > Malware Protection**.

### Action (Available only if Scanning is enabled)

Enable action to be taken on the mails received, from the available options:  
**Quarantine:** If enabled, copies the Email to the quarantine file list. Email is either delivered to recipient or dropped, as per configured **Recipient Action**. You can view the Email details like sender and receiver of the Email in the **Quarantine**. Administrator can access the Quarantine from **Email > SMTP Quarantine** while user can access from their respective User Portal.  
**Notify Sender:** If enabled, the original message is withheld by the Device and a notification is sent to the sender informing that the Email was infected. The sender will receive the notification only if the Receiver Action is configured as Don't Deliver.

**Default - Disable**

## Delivery Option for Infected Attachment/Protected Attachment (Available only if Scanning is enabled)

### Recipient Action

Select the action to be taken on the message that is detected to be Infected, Suspicious or includes a Protected Attachment.

#### Available Options:

Don't Deliver: Receiver will not receive the message and will also not receive the notification regarding the infected Email.Deliver Original: Receiver receives the original Email.Remover and Deliver: Infected part of the Email is removed before delivering. Receiver will also receive the notification stating that the Email was infected and infected portion of the Email is removed. Not applicable for Blocked Attachments (Block File Type).



**Note:** Protected attachments are not scanned but receiver will be notified, if not specified otherwise.

### Notify Administrator

Select the action to notify the Administrator for the message detected to be Infected, Suspicious or includes a Protected Attachment.

#### Available Options:

Don't Deliver: Administrator will not be notified about the infected Email.Send Original: Administrator receives the original Email.Remove Attachment: Recipient receives message without attachment and the Administrator receives the notification that the Email attachment was infected and removed before delivering Email.



**Note:** Protected attachments are not scanned but receiver will be notified, if not specified otherwise.

Scanning	Enable <input type="button" value="▼"/>	
Action	<input type="checkbox"/> Quarantine <input type="checkbox"/> Notify Sender	
Delivery Option for	Infected Attachment	Protected Attachment
Recipient	Don't Deliver <input type="button" value="▼"/>	Don't Deliver <input type="button" value="▼"/>
Administrator	Don't Deliver <input type="button" value="▼"/>	Don't Deliver <input type="button" value="▼"/>

**Figure 426: Malware Filter**

6. Click Save.

### Add SMTP Spam Scan Policy

SMTP Spam Scan policies appear only when Legacy mode is enabled. The device acts as a transparent proxy.

This feature requires a subscription. It can be configured but cannot be enforced without a valid Email Protection subscription.

The Add SMTP Scan Policy page allows you to configure scanning policy to detect incoming and outgoing spam in email traffic and take appropriate action.

1. Go to Email > Policies, click Add Policy and then click **SMTP Spam Scan**.

2. Enter a **Name** for the policy.
3. Enter Email Address/Domain Group details.

#### **Sender**

Specify Email Address(es) of the Sender(s). You can select from:

Contains: Specify keywords to be matched with Sender Email Addresses. The rule applies to Address(es) containing those keywords. For example, if the keyword “mail” is specified, the rule will apply to Sender Email Addresses john@hotmail.com, sophosmail@sophos.com, etc.

Equals: Specify the exact Email Address(es) of the Sender(s).

You can also add RBLs, a list of Email Addresses or keywords using the **Create New** link.

#### **Recipient**

Specify Email Address(es) of the Recipient(s). You can select from:

Contains: Specify keywords to be matched with Recipient Email Addresses. The rule applies to Address(es) containing those keywords. For example, if keyword “mail” is specified, the rule will apply to Recipient Email Addresses john@hotmail.com, sophosmail@sophos.com, etc.

Equals: Specify the exact Email Address(es) of the Recipient(s).

You can also add RBLs, a list of Email Addresses or keywords using **Create New** link.

Sender *	Contains	Any
Recipient *	Contains	Any

**Figure 427: Email Address/Domain Group**

4. Select the Filter Criteria.

#### **Inbound Email is**

All the Emails that are received by the users in their inbox are referred to as Inbound.

If you select Inbound Spam, all the Emails received by the users are scanned for spam and viruses by the Device.

The specified action will be taken if the Device has identified the Inbound Email to be one of the following:

Spam Probable Spam Virus Outbreak Probable Virus Outbreak

#### **Outbound Email is**

Emails that are sent by the user in the network to a remote user on another Email system, are referred as Outbound.

If you select Outbound Spam, all the Emails sent by the local users are scanned for spam and viruses by the Device before being delivered.

The specified action will be taken if the Device has identified the Outbound Email to be one of the following:

Spam Probable Spam Virus Outbreak Probable Virus Outbreak

#### **Source IP/Network Address**

Specify the action to be taken when the Email sender IP Address matches the specified IP Address.

#### **Destination IP/Network Address**

Specify the action to be taken when the Email recipient IP Address matches the specified IP Address.

#### **Sender Remote Blacklist**

Specify the action to be taken when the sender is listed in the specified RBL Group.

#### **Message Size**

The specified action will be taken if the Email size matches the specified size.

#### **Message Header**

The specified action will be taken if the message header equals or contains the specified text.

Contains: Specify keywords to be matched with Message Header. The rule applies to Header(s) containing those keywords.

Equals: Specify the exact Header(s) to be scanned.

#### **You can scan message header for Spam in:**

Subject: The specified action will be taken if the header contains the matching subject. From: The specified action will be taken if the header contains the matching text in the From address. To: The specified action will be taken if the header contains the matching text in the To address. Other: The specified action will be taken if the matching text is found in the headers.

#### **Data Control List**

The specified action will be taken if the message contains data matching with the configured [Data Protection Policy](#). You can create Data Protection Policies at **Email > Data Control List**.



**Note:** Data Protection is applicable on outbound emails only.

#### **None**

Select this to create a rule for email between a specific sender and recipient without any conditions. You can set actions for SMTP/S and POP/S-IMAP/S mails only on the basis of sender and recipient.

The screenshot shows the 'Filter Criteria' section of the Sophos XG Firewall configuration. It lists several filter types with their respective settings:

- Inbound Email is:** Set to 'Spam'.
- Outbound Email is:** Set to 'Spam'.
- Source IP/Network Address:** An empty list with an 'Add New Item' button.
- Destination IP/Network Address:** An empty list with an 'Add New Item' button.
- Sender Remote Blacklist:** Set to 'RBL Group'.
- Message Size:** Set to 'Greater Than' with a value field.
- Message Header:** Set to 'Select Message Header' with a value field.
- Data Control List:** Set to 'Contains' with a value field.
- None:** Set to 'None'.

**Figure 428: Filter Criteria**

## 5. Select the Action.

### Action

Select action to be taken for the SMTP/S traffic.

#### Available Options:

Reject: Email is rejected and a rejection notification is sent to the Email sender. Accept (*Not available for Outbound Spam*): Email is accepted and delivered to the intended recipient. The Administrator can bind an SPX Template to this action so that the Email is delivered to the intended recipient after being SPX-encrypted.



**Note:** SPX Encryption is applicable on outbound emails only.

Change Recipient: Email is accepted but is not delivered to the intended recipient for whom the message was originally sent. Email is sent to the recipient specified in the spam policy. Prefix Subject (*Not available for Outbound Spam*): Email is accepted and delivered to the intended recipient but after tagging the subject line. The Administrator can bind an SPX Template to this action so that the Email is delivered to the intended recipient after being SPX-encrypted. Tagging content is specified in the **To** field. You can customize subject tagging in such a way that the recipient knows that the is a spam Email. For Example, Contents to be prefixed to the original subject: "Spam notification from the Device –" Original subject: "This is a test" Recipient will receive Email with the subject line: "Spam notification from the Device - This is a test" Drop: Email is rejected but a rejection notification is not sent to the Email sender.

### SPX Template

If the action selected is **Accept**, **Prefix Subject** or **Accept with SPX**, select the SPX Template to be applied to the Email. You can create **SPX Template** from **Email > Encryption**.



**Note:** SPX Encryption is applicable on outbound emails only.

## Quarantine

If this is enabled, the device does not deliver Email but copies it to the quarantine file list. You can view the Email details like the sender and recipient in the quarantined file list.

6. Click Save.

### Related tasks

[Add SPX Templates](#) on page 474

[Add a Data Control List](#) on page 470

## Add POP-IMAP Scan Policy

This feature requires a subscription. It can be configured but cannot be enforced without a valid Email Protection subscription.

Add a POP-IMAP scan policy to detect incoming and outgoing spam in POP/S and IMAP/S traffic.

1. Go to **Protect > Email > Policies** and click **Add Policy**. Click **POP-IMAP Scan**.
2. Enter a **Name** for the policy.
3. Enter email address or domain group details.

### Sender

To specify the sender email addresses, select from the following options:

Contains: Specify the keywords to be matched with the senders' email addresses. Example: If you specify the keyword mail, the rule applies to senders' email addresses such as example@examplemail.com, sophosmail@example.com.

Equals: Specify the senders' exact email addresses.

To add a list of keywords or email addresses, click **Create New**.

### Recipient

To specify the recipient email addresses select from the following options:

Contains: Specify the keywords to be matched with the recipient email addresses. Example: If you specify the mail, the rule applies to recipient email addresses such as example@examplemail.com, sophosmail@example.com.

Equals: Specify the recipients' exact email addresses.

To add a list of keywords or email addresses, click **Create New**.

**Figure 429: Email Address/Domain Group**

4. Select from the following **Filter Criteria** based on which the specified action is to be taken:

### Inbound Email is

Select from the following options:

Spam Probable Spam Virus Outbreak Probable Virus Outbreak

#### Source IP/Network Address

Sender's IP address matches the specified IP address.

#### Message Size

Sender's email size matches the specified restriction of message size.

#### Message Header

Select from the following message headers to match the specified keyword:

Subject From To Other

Select the type of keyword match from the following options:

Contains: Specify the keywords to be matched with the message header.

Equals: Specify the exact match to the actual headers.

#### None

Select to create a policy between specific senders and recipients without imposing any other condition.

<input checked="" type="radio"/> Inbound Email is	Spam
<input type="radio"/> Source IP/Network Address	
<input type="radio"/> Message Size	Greater Than
<input type="radio"/> Message Header	Select Message Header Contains
<input type="radio"/> None	

**Figure 430: Filter Criteria**

5. Select the action.

#### Action

Action to be taken from the following options:

##### Available Options:

Accept: Email is accepted and delivered to the intended recipient. Prefix Subject: Email is accepted and delivered to the intended recipient after adding a prefix to the subject line. Specify the prefix in the **To** field. You can set the prefix to indicate the filter criteria.

Example:

Original subject line: Test mail

Tagged content: Probable Spam

Recipient receives email with the subject line: 'Probable Spam: Test mail'

6. Click Save.

#### Data Control List

**This feature requires a subscription. It can be configured but cannot be enforced without a valid Email Protection subscription.**

**This feature is available in Cyberoam Models CR15iNG and above, and all Sophos UTM and Sophos Firewall Models.**

You can create a Data Control List of confidential data by selecting from the Content Control List (CCL). The device provides CCLs based on expert definitions for common financial and personally identifiable data types (example: credit card and social security numbers, postal and email addresses).

Subsequently, you can use Data Control Lists to set Data Protection for emails.

#### Related concepts

[Quarantine Digest](#) on page 459

#### Add a Data Control List

**This feature requires a subscription. It can be configured but cannot be enforced without a valid Email Protection subscription.**

**This feature is available in Cyberoam Models CR15iNG and above, and all Sophos UTM Models.**

**Add Data Control List** allows you to create a list of confidential data types. The device provides Content Control Lists (CCL) based on expert definitions for common financial and personally identifiable data types.

1. Go to **Protect > Email > Data Control List** and click **Add**.
2. Enter the name.
3. Select the CCLs (Content Control List) from the list. Filter the CCLs based on **Type** and **Region**.

**Figure 431: Data Control List**

4. Click **Save**.

#### Related tasks

[Add SMTP Spam Scan Policy](#) on page 464

#### SMTP Quarantine

**SMTP Quarantine is available only in Sophos Firewall XG105, Cyberoam CR2SiNG, Sophos UTM SG105, and higher models.**

**This feature requires a subscription. It can be configured but cannot be enforced without a valid Email Protection subscription.**

The **SMTP Quarantine** allows you to filter the quarantined emails. The page displays all the emails quarantined by the device if they are found to be:

- From a blocked Source IP Address
- Destined to a blocked Destination IP Address
- Virus-infected
- Oversized
- Containing a Blocked Header
- Containing unscannable content or a protected attachment
- blocked by an RBL
- blocked by a Data Protection (DP)
- Spam
- Found malicious by Sandstorm
- quarantined due to any other reason

Use the filter to search for mails from the list of quarantined emails.

The filter result displays a list of all the quarantined emails based on the filter criteria.

**Total utilization** displays the percentage of the quarantine area used by quarantined emails. Once the quarantine repository is full older emails are purged.

### Quarantine Digest

The Quarantine Digest is an email containing a list of quarantined emails filtered by the device and held in the user's quarantine area. If configured, the user receives a Quarantine Digest as per the frequency set in **Email > Quarantine Digest**. The digest also provides a link to the User Portal from where the user can access quarantined emails and take the required action.

### Releasing Quarantined Email

Either the Administrator or the user can release the quarantined Emails. Administrator can release the quarantined Emails from the Quarantine Area while the user can release them from his User Portal. Released quarantined Emails are delivered to the intended recipient's inbox. The Administrator can access the Quarantine Area from **Email > SMTP Quarantine**, while user can log on to the User Portal and access the Quarantine Area from **SMTP Quarantine**. If Quarantine Digest is configured, user will receive Digest of the quarantined mails as per the configured frequency.

#### Note:

- Virus-infected emails and the emails found malicious by Sandstorm cannot be released.
- To delete Sandstorm related emails, you need Read-Write permission for Sandstorm Activity.

Start Date	2016-12-16	End Date	2016-12-16
Sender	<input type="text"/>	Recipient	<input type="text"/>
Subject	<input type="text"/>		
Filter By	<input checked="" type="checkbox"/> Blocked Source IP <input checked="" type="checkbox"/> Oversized Message <input checked="" type="checkbox"/> Blocked by RBL <input checked="" type="checkbox"/> Spam <input checked="" type="checkbox"/> Blocked Destination IP <input checked="" type="checkbox"/> Blocked Header <input checked="" type="checkbox"/> Blocked by Data Protection <input checked="" type="checkbox"/> Analyzed by Sandstorm <input checked="" type="checkbox"/> Infected <input checked="" type="checkbox"/> Unscannable Content/Protected Attachment <input checked="" type="checkbox"/> Other		
<input type="button" value="Filter"/> <input type="button" value="Clear"/>			

**Figure 432: SMTP Quarantine**

## Encryption

**SPX Encryption is available in Sophos Firewall XG105 and higher models, Cyberoam CR25iNG and higher models, and all Sophos UTM Models.**

**This feature requires a subscription. It can be configured but cannot be enforced without a valid Email Protection subscription.**

### What is SPX Encryption?

SPX (Secure PDF Exchange) encryption is a next-generation version of email encryption. It is clientless and extremely easy to set up and customize in any environment. Using SPX encryption, email messages and any attachments sent to the Device are converted to a PDF document, which is then encrypted with a password. You can configure the Device to allow senders to select passwords for the recipients, or the server can generate the password for the recipient and store it for that recipient, or the server can generate one-time passwords for recipients.

When SPX encryption is enabled, there are two ways in which emails can be SPX encrypted:

- The user can download the Sophos Outlook Add-in from **User Portal**. After having it installed, an Encrypt button is displayed in the Microsoft Outlook user interface. To encrypt a single message, the user needs to click the Encrypt button and then write and send the message.



#### Note:

If you do not use Outlook you can also trigger SPX encryption by setting the header field X-Sophos-SPX-Encrypt to “yes”.

- In the Data Protection feature, you can enforce SPX encryption of Emails containing sensitive data (see **Email > Policies > SMTP Policy**).

The encrypted message is then sent to the recipient’s mail server. Using any PDF reader, the recipient can decrypt the message with the password that was used to encrypt the PDF. SPX-encrypted email messages are accessible on all popular smartphone platforms that have native or third-party PDF file support, including Android, iOS, Blackberry and Windows Mobile devices.

The SPX-encrypted email contains a **Reply** button which links to the SPX Reply Portal. Using the SPX Reply Portal, the recipient is able to answer to the email in a secure way.

## SPX Configuration

### Default SPX Template

Select the SPX Template to be used by default. The Default Template is used if any user explicitly SPX-encrypts an email and no template is selected in the Content Scanning Rule.

The user can SPX-encrypt an Email by:

- Manually setting the Email header **X-Sophos-SPX-Encrypt** to “yes”.
- Installing the Sophos Outlook Add-on and clicking **Encrypt** before sending the Email.

If the Default SPX Template is set to **None**, then SPX encryption is not applied to Email.

### Keep Unused Password for

Enter the expiry time in days of an unused password.

For example, if Keep Unused Password for is set to 3 days, the password will expire at 0 o’clock 3 days after being generated if no SPX encrypted message has been sent for a specific recipient.

Default: 30 days

### Allow Password Registration for

Enter the time in days after which the link to Password Registration Portal expires.

Default: 10 days

### Send Error Notification To

Specify whom to send a notification when an SPX error occurs. You can send the notification to the sender or you can send no notification at all. Error messages will always be listed in the SMTP log.

Default SPX Template	Default Template	<input type="button" value="▼"/>
Keep Unused Password for	30	Day(s)
Allow Password Registration for	10	Day(s)
Send Error Notification to	Sender Only	<input type="button" value="i"/>

**Figure 433: SPX Configuration**

### SPX Portal Settings

#### Hostname

Enter the IP Address or Domain on which the Password Registration Portal is hosted.

#### Allowed Network(s)

Enter the networks from which password registration requests will be accepted.

#### Port

Enter the port on which the SPX Password Registration Portal should listen.

Default: 8094

Hostname	None	<input type="button" value="▼"/>
Allowed Network(s)	Any	<input type="button" value="–"/>
	Add New Item	
Port	8094	

**Figure 434: SPX Portal Settings**

### SPX Password Reset

#### Reset Password for

Enter the Email Address for the recipient for whom you want to reset the password. New SPX email to this address requires the recipient to obtain a new password from the sender.

Reset Password for	Enter Email Address	<input type="button" value="Reset"/>
--------------------	---------------------	--------------------------------------

**Figure 435: Password Reset**

## SPX Templates

The SPX template defines the layout of the PDF file, password settings and recipient instructions. You can also define different SPX templates. So, if you are managing various customer domains, you can assign them customized SPX templates containing, for example, different company logos and texts.

This page allows you to add, edit and delete SPX templates.

Name	Password Type	
Default Template	Specified by sender	

**Figure 436: SPX Templates**

### Add SPX Templates

**SPX Encryption is available in Sophos Firewall XG105 and higher models, Cyberoam CR25iNG and higher models, and all Sophos UTM Models.**

**This feature requires a subscription. It can be configured but cannot be enforced without a valid Email Protection subscription.**

This page allows you to define new SPX Templates or modify existing templates.

1. Go to **Protect > Email > Encryption > SPX Templates** and click **Add**.
2. Enter parameter values for the following basic settings.

#### Name

Specify the name to uniquely identify the template. The name should be a string containing alphanumeric and special characters EXCEPT forward slash (/), backslash (\), comma (,), double quote ("") and single quote (').

#### Description

Specify details of the template.

#### Organization Name

Specify the organization name to be displayed on notifications concerning SPX sent to the administrator or the email sender, depending on your settings.

#### PDF Encryption

Select the encryption standard of the PDF file.

#### Page Size

Select the page size of the PDF file.

Name *	<input type="text"/>
Description	<input type="text"/>
Organization Name	<input type="text"/>
PDF Encryption	AES / 128
Page Size	A4

**Figure 437: General Settings**

3. Enter Password Settings.

#### Password Type

Select how you want to generate the password for accessing the encrypted email message. The sender always has to take care of transferring the password in a safe way to the recipient, unless you select **Specified by recipient**.

##### Available Options:

###### Specified by Sender:

If you select this, the email sender should provide the password. The sender has to enter the password into the Subject field, using the following format:

[secure:<password>]<subject text> where <password> is the password to open the encrypted PDF file and <subject text> is the random subject. Of course, the password will be removed by the Device before the email is sent to the recipient.

###### Generated one-time password for every email:

The Device automatically creates a new password for each affected email. An email notification is mailed to the sender containing instructions and the one-time generated password.

The HTML content of this Email can be customized from **Notification Subject** and **Notification Body**. You can reset to the default content by clicking **Reset** .

###### Generated and stored for recipient:

The Device automatically creates a recipient-specific password when the first email is sent to a recipient. This password will be sent to the sender. With the next email, the same password is used automatically. The password will expire when it is not used for a configured time period, and it can be reset by the administrator, see [Encryption](#).

The HTML content of this Email can be customized from **Notification Subject** and **Notification Body**. You can reset to the default content by clicking **Reset** .

###### Specified by recipient:

If you select this, the email recipient should provide the password. The recipient receives an email notification containing a link leading to the Password Registration Portal to register a password and the Sender receives a failure notification. After registration, the recipient is able to view the current encrypted mail and any future encrypted mails using the same password from this or other senders from the same organization.



**Note:** The Recipient's password generated via **Specified by recipient** method and **Generated and stored for recipient** are mutually exclusive. The recipient will have to use the respective password when email is received after SPX Encryption using different methods.

**Figure 438: Password Settings**

#### 4. Specify Recipient Instructions:

##### Instructions for Recipient

The body of the email that is sent from the Device to the email recipient containing instructions concerning the encrypted email. Simple HTML markup and hyperlinks are allowed. You can also use variables, e.g.,

%%ORGANIZATION\_NAME%%



**Tip:** The Default SPX Template on this tab contains all available variables and gives a useful example of recipient instructions. The variables used are:

- ENVELOPE\_TO: The recipient for whom the password is generated.
- PASSWORD: The password to open SPX encrypted Email
- ORGANIZATION\_NAME: The name provided in the **Organization Name** field.
- SENDER: The sender of the email.
- REG\_LINK: The link to the Registration Portal for registering the password.

Instructions for recipient

```
<p><b>Encrypted email notification from %ORGANIZATION_NAME%</b></p>
<p><b>Encrypted email message from %SENDER%</b></p>

<p>This email contains a message that has been sent as an encrypted PDF document in order to ensure the secure delivery of its contents.</p>

<font size="+1"><b>Open the encrypted PDF attachment to view your secure message.</b></font>

<p>To access this message, you should open the attached PDF using Adobe Acrobat Reader version 7.0 or <a href="#">another supported reader</a>.</p>
```

**Figure 439: Recipient Instructions**

#### Related tasks

[Add SMTP Spam Scan Policy](#) on page 464

#### General Settings

This feature requires a subscription. It can be configured but cannot be enforced without a valid Email Protection subscription.

Email Configuration allows you to configure the general settings Email traffic. This page contains the following sections.

#### SMTP Deployment Mode

MTA mode is available only in Sophos Firewall XG105, Cyberoam CR25iNG, Sophos UTM SG105, and higher models.

Click button to switch to MTA/Legacy Mode.

In MTA Mode, Device acts as a Mail Transfer Agent (MTA). In Legacy Mode, Device acts as a transparent proxy.

When acting as an MTA, Device is responsible for routing Emails to and from the protected Email Server(s). In this state Device allows you to:

- configure relay of inbound and outbound Emails from **Email > Relay Settings**.
- set up multiple SMTP Profiles to protect multiple Domains on your internal Email Server or multiple Email Servers from **Email > Policies > SMTP Policies**.
- view email messages that are either waiting for delivery or have produced an error in the **Email > Mail Spool**.
- view the logs for all the emails processed by the Device from **Email > Mail Logs**.

Default: MTA Mode is enabled.



#### Note:

- On enabling MTA Mode, a firewall rule to allow SMTP/SMTPS traffic is automatically created.
- If you have migrated from CyberoamOS to SFOSv16 OR SFOSv15 to SFOSv16, Legacy Mode will be enabled by default.

**Device acts as a Transparent Proxy.**

You can switch to MTA Mode wherein Device acts as a Mail Transfer Agent (MTA).

**Switch to MTA Mode**

**Figure 440: SMTP Deployment Mode**

### Banner Settings

#### Append Banner to All Outbound Messages

Enable to add a banner at the end of all outgoing Email messages.

The banner is appended ONLY when SMTP and SMTPS Scanning is enabled in the relevant Business Application Policy(s).

#### Email Banner

Specify a banner to be added to all outgoing Emails. Only text banners are allowed.

Example:

*This email contains confidential information. You are not authorized to copy the contents without the consent of the sender. Please do not print this email unless it is absolutely necessary. Spread environmental awareness.*

**Banner Settings**

Append Banner to All Outbound Messages  OFF

Email Banner

**Figure 441: Banner Settings**

## SMTP Settings

### SMTP Hostname

Specify the SMTP hostname to be used in HELO and SMTP banner strings. By default, Device uses 'Sophos' as hostname.



**Note:** For Legacy Mode, this hostname is applicable only to system-generated notification emails.

### Don't Scan Emails Greater Than

Specify maximum file size (in KB) for scanning. Files exceeding this size received through SMTP/S will not be scanned.

Default - 1024 KB

Specify 0 to increase the default file size scanning restriction to 51200 KB.

### Action for Oversize Email

Specify the action for Oversize Emails.

#### Available Options

Accept: All the oversize mails are forwarded to the recipient without scanning. Reject: All the oversize mails are rejected and sender is notified. Drop: All the oversized mails are dropped, without notifying the sender.

### Bypass Spam Check for SMTP/S Authenticated Connections (Available in Legacy Mode only)

Enable to bypass Spam Scanning for Email messages received over SMTP/S connections authenticated by the Email Server.

### Verify Sender's IP Reputation

Click to verify the reputation of the sender IP Address. When enabled, the Device dynamically checks the sender's IP Address of all Emails. If the IP Address is found to be responsible for sending spam email or malicious contents, the Device takes action as per the configured Scanning Rules.

If enabled, specify an action for Confirmed Spam Emails and Probable Spam Emails.

#### Available Options

Accept: All the spam Emails are forwarded to the recipient after scanning as per the configuration. Reject: All the spam mails are rejected and a notification is sent to the Email sender. Drop: All the spam mails are dropped, without notifying the sender.

As it is a global option, if spam scanning is enabled, all the mails will first be subjected to IP Reputation filtering followed by filtering based on actions configured in the spam policy.

Default - Disable

## SMTP DoS Settings

Enable to configure SMTP DoS Settings which protect the network from SMTP DoS Attacks.

If this is enabled, specify values for Maximum Connections, Maximum Connections/Host, Maximum Emails/Connection, Maximum Recipients/Email, Email Rate per Minute/Host and Connections Rate per Second/Host.

### Maximum Connections (Available if SMTP DoS Settings Enabled)

Specify maximum number of connections that can be established with the Email Server.

Default - 1024

Acceptable Range - 1 - 20000

### Maximum Connections/Host (Available if SMTP DoS Settings Enabled)

Specify maximum number of connections allowed to the Email Server from a particular host.

Default - 64

Acceptable Range - 1 - 10000

**Maximum Emails/Connection (Available if SMTP DoS Settings Enabled)**

Specify maximum number of Emails that can be sent in a single connection.

Default - 512

Acceptable Range - 1 - 1000

**Maximum Recipients/Email (Available if SMTP DoS Settings Enabled)**

Specify maximum number of recipients for a single Email.

Default - 100

Acceptable Range - 1 - 256

**Email Rate per Minute/Host (Available if SMTP DoS Settings Enabled)**

Specify number of Emails to be sent from a particular host in one minute.

Default - 512

Acceptable Range - 1 - 20000

**Connection Rate per Second/Host (Available if SMTP DoS Settings Enabled)**

Specify number of connections allowed to the Email Server from a particular host in one second.

Default - 8

Acceptable Range - 1 - 20000

SMTP Hostname	<input type="text" value="Sophos"/>	This will be used in HELO string for system-generated notification emails.
Don't Scan Emails Greater Than *	<input type="text" value="0"/>	KB Enter 0 for default size restriction of 51200 KB
Action for Oversize Emails *	<input checked="" type="radio"/> Accept <input type="radio"/> Reject <input type="radio"/> Drop	
Bypass Spam Check For SMTP/S Authenticated Connections	<input type="checkbox"/>	
Verify Sender's IP Reputation	<input checked="" type="checkbox"/> Enable	
Confirm Spam Action	<input type="text" value="Reject"/>	
Probable Spam action	<input type="text" value="Reject"/>	
SMTP DoS Settings	<input checked="" type="checkbox"/> Enable	
Maximum Connections *	<input type="text" value="5000"/>	
Maximum Connections/Host *	<input type="text" value="100"/>	
Maximum Emails/Connection *	<input type="text" value="1000"/>	
Maximum Recipients/Email *	<input type="text" value="100"/>	
Emails Rate *	<input type="text" value="1000"/>	Per Minute/Host
Connections Rate *	<input type="text" value="100"/>	Per Second/Host

**Figure 442: SMTP Settings**

## POP/S and IMAP/S Settings

### Don't Scan Emails Greater Than

Specify maximum file size (in KB) for scanning. Files exceeding this size received through POP/IMAP will not be scanned.

Default - 1024 KB

Specify 0 to increase the default file size restriction to 10240 KB.

### Recipient Headers

Specify Header value to detect recipient for POP3/IMAP.

Default - Delivered-To, Received, X-RCPT-TO

Don't Scan Emails Greater Than \*  KB Enter 0 for default size restriction of 10240 KB

Recipient Headers

Headers	
Delivered-To	
Received	
X-RCPT-TO	

**Figure 443: POP/S and IMAP/S Settings**

## SMTP TLS Configuration

### TLS Certificate

Select the CA Certificate or Server Certificate for scanning SMTP traffic over SSL from the available options.

### Available Options

Default ApplianceCertificate SecurityAppliance\_SSL\_CA List of custom CA Certificates and Server Certificates, if added. You can create the custom CA Certificate from **Certificates > Certificate Authorities** and custom Server Certificate from **Certificates > Certificates**.

### Allow Invalid Certificate

If enabled, SMTP over SSL connections will be allowed with an invalid certificate from the Email Server. Disable this option to reject such connections.

Default - Enable

### Require TLS Negotiation with Host/Net

Select the remote host (Email Server) or network from available options on whose connections TLS encryption is to be enforced. In other words, the Device will always initiate TLS-secured connections when Emails are to be sent to selected hosts/networks. If TLS is enforced but connection cannot be established, then Emails to that remote host/network are discarded.

### Require TLS Negotiation with Sender Domain

Specify the Sender Domain(s) on whose Email connections TLS encryption is to be enforced.

Sender Domain is the domain of the Email sender. Emails from the specified Sender Domain will be sent over TLS-encrypted connections only. If TLS is enforced but connection cannot be established, then Emails from that sender domain are discarded.

### Skip TLS Negotiation Hosts/Nets

Select the remote host (Email Server) or network from available options on whose connections TLS encryption is to be skipped or bypassed. When configured, SMTP connections to selected hosts will be established in clear text and unencrypted.

TLS Certificate *	<input type="text" value="SecurityAppliance_SSL_CA"/> 
Allow Invalid Certificate	<input checked="" type="checkbox"/> Enable
Require TLS Negotiation with Host/Net	<input type="button" value="Add New Item"/>
Require TLS Negotiation with Sender Domain	<input type="button" value="Add New Item"/>
Skip TLS Negotiation Hosts/Nets	<input type="button" value="Add New Item"/>

**Figure 444: SMTP TLS Configuration****POP and IMAP TLS Configuration****TLS Certificate**

Select the CA for scanning POP and IMAP traffic over SSL from the available options.

**Available Options**

DefaultSecurityAppliance\_SSL\_CAList of custom CAs if added. You can create the custom CA from **Certificates > Certificate Authorities**.

**Allow Invalid Certificate**

If enabled, POP and IMAP over SSL connections will be allowed with invalid certificate from the Mail Server. Disable to reject such connections.

Default - Enable

TLS Certificate *	<input type="text" value="SecurityAppliance_SSL_CA"/> 
Allow Invalid Certificate	<input checked="" type="checkbox"/> Enable

**Figure 445: POP and IMAP TLS Configuration****Email Journaling (Available in Legacy Mode only)**

Email being one of the most important communication and business tools in use by organizations, email journaling has become an integral part of every organization.

Using the Device's Email Journaling, the administrator can store all incoming Emails, or Emails for a specific recipient or a group of recipients and thereby keep a close watch over data leakage.

The device can journal all Emails intended for single or multiple recipients and can forward them to a single administrator or multiple administrators.

This section displays a list of the archivers created and provides options to [add a new archiver](#), [update the parameters of existing archiver](#), or delete the archiver. You can filter the list based on recipient name.

<input type="checkbox"/> Name	Recipient	Send Copy To	Manage
No Records Found			

**Figure 446: Email Journaling**

### Spam Check Exceptions

To bypass spam scanning of certain domains, define the domains as Spam Check Exceptions. The page lists all the domains configured to be exempted from spam scanning.

It also provides the options to add a new domain and delete an existing domain.

Domain Name \*

**Add**

<input type="checkbox"/> Domain Name	Manage	Delete
No Records Found		

**Figure 447: Spam Check Exceptions**

### Malware Protection

**Malware Protection is available in Sophos Firewall XG105, Cyberoam CR500iNG, Sophos UTM SG105, and higher models.**

Sophos Firewall offers dual anti-virus scanning, wherein traffic is scanned by two (2) anti-virus engines. Traffic is first scanned by the primary engine, and then by the secondary engine.

#### Primary Anti Virus Engine

Select the primary anti-virus engine for traffic scanning. For dual scan, packets are first scanned by the primary engine and then by the secondary engine. For single scan, only the primary engine is used.

#### Available Options

SophosAvira

**Note:** Selecting **Avira** will disable Sandstorm in all SMTP Policies with Single Anti-Virus Scanning.

Primary Anti-Virus Engine

Sophos

**Apply**

**Figure 448: Malware Protection**

## Smarthost Settings

A smarthost is a Mail Transfer Agent (MTA) which acts as an intermediate server between the sender's and recipient's email servers. On configuring a smarthost, the device redirects outbound emails to the designated server, which are then routed to the recipient's email server.

Enable **Use Smarthost**.

### Hostname

Select the host that will act as a smarthost.



**Note:** You cannot configure Smarthost as the device's interface IP address. It will result in a routing loop.

### Port

Enter the port.

Default: 25

### Authenticate Device with Smarthost

Select if the smarthost requires the device to authenticate before routing emails. Both Plain and Login authentication types are supported. Enter a **Username** and **Password**.

The screenshot shows the 'Smarthost Settings' configuration page. At the top left is a checked checkbox labeled 'Use Smarthost'. Below it is a 'Hostname' field containing an empty input box and a 'Port' field containing the value '25'. Underneath these are two more checkboxes: 'Authenticate Device with Smarthost' (which is also checked) and 'Plain' (which is unchecked). To the right of the 'Plain' checkbox is a 'Password' field with a redacted password and a 'Change Password' link. At the bottom left is a blue 'Apply' button.

**Figure 449: Smarthost Settings**

### Advanced SMTP Settings (Available in MTA Mode only)

#### Reject invalid HELO or missing RDNS

Select this option if you want to reject hosts that send invalid HELO/EHLO arguments or lack RDNS entries. Select **Do strict RDNS checks** if you want to additionally reject email from hosts with invalid RDNS records. An RDNS record is invalid if the found hostname does not resolve back to the original IP address.

### Scan Outgoing Mails

Enable to scan all outgoing email traffic. Email is quarantined if found to be malware infected, or marked as Spam.

The screenshot shows a configuration panel for SMTP settings. It contains two sections: 'Reject invalid HELO or missing RDNS' (unchecked) and 'Scan Outgoing Mails' (checked). Each section has an 'i' icon for more information. At the bottom is a prominent blue 'Apply' button.

**Figure 450: Advanced SMTP Settings**

### Add Email Journal

**Email Journal is available only in Legacy mode (device acts as transparent proxy).**

**This feature requires a subscription. It can be configured but cannot be enforced without a valid Email Protection subscription.**

**Add Email Journal** allows you to forward copies of emails of specific recipients to a different email address, for example, to an administrator.

1. Go to **Protect > Email > General Settings** and click **Add** under **Email Journaling**.
2. Enter a name.
3. In the **Recipient** box, select **Any** to journal all incoming emails. Alternately, select the address groups, copies of whose emails are to be forwarded to a different email address.
4. In the **Send Copy Of Email To** box, enter the email address to which a copy of emails is to be forwarded.
5. Click **Save**.

The screenshot shows a form for creating a new email archiver entry. It includes fields for 'Name \*' (with a placeholder 'Enter Name'), 'Recipient \*' (set to 'Any'), and 'Send Copy Of Email To \*' (with a note '(Applicable To SMTP/S Only)').

**Figure 451: Email Archiver**

### Address Groups

Policies are applied on Email Addresses. To make configuration easier and simpler, the Administrator can group the addresses that require the same scanning policy. The policy applied to the address group is applicable to all the group members. Hence when the group is used in a number of rules, it becomes much easier to add or remove addresses from the group rather than updating individual rules. Hence, just with the one update, the Administrator can re-align the rules.

An Address Group is a grouping by:

- Email Address or Domain
- IP Address
- RBL (Real time black hole List) (applicable only for the spam email)

An address can be a member of multiple groups.

An RBL is a list of IP Addresses whose owners are responsible for spam or are hijacked for a spam relay. These IP Addresses might also be used for spreading viruses. The Device checks each RBL for the connecting IP Address and

the action configured in the policy is taken if the IP Address is found in any of the RBL lists. The Administrator can directly use the two default RBL groups shipped with the Device or update them as per their requirement:

- Premium RBL Services
- Standard RBL Services

The Address Group page displays a list of all the default and custom groups and provides options to add a new group, update the parameters, import addresses in the existing group, or delete the group. You can sort the list based on address group name.

### Add Address Group

1. Go to **Protect > Email > Address Group** and click **Add**.
2. Enter a name and description.
3. **Group Type:** Select to add email addresses or domains to the address group.

#### Available Options:

##### RBL (IPv4) or RBL(IPv6):

Select to add RBLs of IPv4 or IPv6 addresses or domain names.

If the connecting IP address is found on the RBL, the device takes the action specified by the relevant policy.

##### Email Address/Domain:

Select to add the email address or domain name.

**Import:** Select to upload a CSV or text file.

**Manual:** Select to add individual email addresses or domains.

#### Note:

- You can import a maximum of 400 email addresses or domains in a single file.
- Invalid and duplicate entries are not imported.

Name *	<input type="text" value="Enter Name"/>
Description	<input type="text" value="Enter Description"/>
Group Type	<input type="radio"/> RBL (IPv4) <input type="radio"/> RBL(IPv6) <input checked="" type="radio"/> Email Address/Domain
Type	<input type="radio"/> Import <input checked="" type="radio"/> Manual
Email Address(es)/Domain(s) *	<input type="text"/> <div style="border: 1px solid #ccc; padding: 5px; display: flex; align-items: center; justify-content: space-between;"> <span>Search / Add</span> <span style="font-size: 2em;">+</span> </div>

**Figure 452: Address Group**

4. Click **Save**.

## File Types

A file type is a classification that is determined by file extension and MIME header. You can include file types in web policies to control access to files that match the specified criteria. The default file types contain some common criteria and you can create additional types.

### Using File Types with Policy Rules

You can create file types to control access to files on a more granular level. For example, you may want to allow access to SQL files but deny access to all other database files. In this case, you would create a file type for SQL files and a policy that specifies the following rules in the following order:

1. Allow access to SQL files
2. Block access to all database files

### Add File Type

1. Go to **Protect > Web > File Type** and click **Add**.
2. Type a name.
3. (Optional) Select a template.

You can select from predefined or custom file types. If you do not wish to use a template, choose **Blank**.

4. Specify the file extension and MIME header.

Name *	<input type="text"/>
Description	<input type="text"/>
Template	<input type="button" value="Blank"/>
File Extension *	<input type="text"/> Add Extensions here <small>Use comma as a separator to enter multiple entries.</small>
MIME Header *	<input type="text"/> Add MIME Headers here <small>Use comma as a separator to enter multiple entries.</small>

**Figure 453: Add File Type**

## Quarantine Digest

**Quarantine Digest** is available only in Sophos Firewall XG105, Cyberoam CR25iNG, Sophos UTM SG105, and higher models.

This feature requires a subscription. It can be configured but cannot be enforced without a valid Email Protection subscription.

**Quarantine Digest** allows you to set the frequency at which the digest email is sent to the user. You can enable or disable user access to quarantined emails on the user portal. You can also enable quarantine digest for all users or to specific users and groups.

Quarantine Digest provides the date and time of message receipt, sender and recipient's email addresses and subject of the message.

## Quarantine Digest Settings for All Users

1. Go to **Protect > Email > Quarantine Digest**.
2. Select **Enable Quarantine Digest** to email the digest to all users.
  - a. Set the **Email Frequency** of the digest. Set the interval, time, and day of week, based on the selection.
  - b. In the **From Email Address** box, enter the address from which the email is to be sent.
  - c. In the **Display Name** box, specify the name of the quarantine digest sender.
  - d. Click **Send Test Email**. Enter the **To Email Address** and click **Send**.
  - e. To set the IP address of the user portal, select the **Reference User Portal IP** from the list.



**Note:** Users located behind the selected port can click the “My Account” link in the digest email to gain access to quarantined emails on the user portal. Others can access the user portal by typing `https://<IP Address of SF Device>` in the browser.

Example: If Port1 is selected as the **Reference User Portal IP**, only users located behind Port1 will be redirected to the user portal when they click on “My Account”.

3. Click **Apply**.

## Override Quarantine Digest Settings for Specific Users

1. Go to **Protect > Email > Quarantine Digest**.
2. Click **Change User’s Quarantine Digest Settings**, to apply the settings to specific users or groups.
3. Select the users or groups.
4. Click **Apply**.

The screenshot shows the 'Quarantine Digest' configuration page. At the top, there is a checked checkbox labeled 'Enable Quarantine Digest'. Below it, there is a section for 'Email Frequency' with three radio buttons: 'Hourly' (unchecked), 'Daily' (checked), and 'Weekly' (unchecked). Under 'Daily', there are dropdown menus for 'Send Email Daily At' with values '10' for hours and '00' for minutes. Next, there is a 'From Email Address' field containing 'admin@sophos.com'. Below that is a 'Display Name' field containing 'Quarantine Digest'. A large blue button labeled 'Send Test Email' is centered below these fields. At the bottom, there is a 'Reference User Portal IP' dropdown menu with 'PortA' selected.

**Figure 454: Quarantine Digest**

### Related concepts

[Data Control List](#) on page 469

## Web Server

Web Server Protection provides facilities to manage and add web servers, define protection policies for them and set up certificates.

The following pages are accessible:

- [Web Servers](#) on page 489: allows you to manage, add and delete settings of web servers connected to your device.
- [Protection Policies](#) on page 490: let you define methods to protect your web servers against malicious attacks.
- [Authentication Policies](#) on page 494: helps to set up authentication policies for direct access to Sophos Firewall.
- [Authentication Templates](#) on page 497: sets up customized HTML login forms.
- [Certificates](#) on page 86: manages certificates for authentication.
- [Certificate Authorities](#) on page 89: manages certificate authorities which issue certificates.
- [Certificate Revocation Lists](#) on page 90: gives an overview of revoked certificates.

## Web Servers

The **Web Servers** menu allows you to add web servers that are to be protected by the WAF.

This page displays all existing web servers. For each web server, the list shows:

### Name

Name of the web server.

### Host

Host name of the web server.

### Type

Type of communication between Sophos XG Firewall and the web server.

## Add Web Server

This page describes how to add a web server that should be protected by the Web Application Firewall (WAF).

1. Go to **Protect > Web Server > Web Servers** and click **Add**.
2. Enter the following:

### Name

Enter a unique name for the web server.

### Description

Enter a description for the web server.

### Host

Add or select a host, which can either be of the type **IP Address** or **FQDN Host**.

[Add IP Host](#) on page 64

[Add an FQDN Host](#) on page 67



**Note:** We recommend using **FQDN Host** because otherwise the host header contains the IP address of the IP host which may lead to problems with some browsers. To transmit the host header of the original HTTP request, enable **Pass Host Header** in the corresponding WAF business application rule.

### Type

Select a server type, that is, whether you want the communication between SF-OS and the web server to be encrypted (HTTPS) or plaintext (HTTP).

Default: Plaintext (HTTP)

### Port

Enter a port number for the web server. By default the standard port of the selected web server type is selected.

### Keep alive

Keeps the connection between SF-OS and the web server open instead of opening a new connection for every single request.

 **Note:** Some web servers do not support keep alive. If you experience reading errors or timeouts, you may need to disable keep alive for the affected server.

### Timeout

Define a connection timeout value, that is the time the WAF waits for data sent by or sent to the web server.

Acceptable range: 1 to 65535 seconds

Default: 300 seconds

Data can be received as long as the web server sends data before the timeout expires. After expiring, the WAF sends an HTTP 502 message to clients.

### Disable backend connection pooling

If enabled, the WAF creates a new connection to the backend server every time it is used, instead of reusing an old connection from the connection pool. This option is disabled by default. Only use it only if you face connection problems because it may decrease system performance.

Name *	<input type="text"/>
Description	<input type="text"/>
Host *	Host
Type	Plaintext (HTTP)
Port *	80
Keep alive	<input checked="" type="checkbox"/> ON
Timeout *	300
Disable backend connection pooling	<input type="checkbox"/> OFF

**Figure 455: Add Web Server**

3. Click Save.

## Protection Policies

The **Protection Policies** menu allows you to define the modes and levels of protection for your web servers.

This page displays all existing web application protection objects. For each protection object, the list shows:  
**Name**

Name of the protection policy.

### Add Protection Policy

This page describes how to add an application protection policy.

1. Go to **Protect > Web Server > Protection Policies** and click **Add**.
2. Specify the following:

#### Name

Enter a unique name for the protection policy.

#### Description

Enter a description for the policy.

## Pass Outlook Anywhere

Enable this to allow external Microsoft Outlook clients to access the Microsoft Exchange Server via the Web Application Protection. Microsoft Outlook traffic will not be checked or protected by the Web Application Protection.

### Mode

Select a mode from the drop-down list:

- **Monitor:** HTTP requests are monitored and logged.
- **Reject:** HTTP requests are rejected.

## Cookie Signing

Enable this to protect a web server against manipulated cookies. When the web server sets a cookie, a second cookie is added to the first cookie containing a hash built of the primary cookie's name, its value and a secret, where the secret is only known by the Web Application Protection. Thus, if a request cannot provide a correct cookie pair, there has been some sort of manipulation and the cookie will be dropped.

## Static URL Hardening

Enable this to protect against URL rewriting. For that, when a client requests a website, all static URLs of the website are signed. The signing uses a similar procedure as with cookie signing. Additionally the response from the web server is analyzed regarding what links can be validly requested next. Moreover, static hardened URLs can furthermore be bookmarked and visited later.



**Note:** Static URL hardening affects all files with a HTTP content type of text/\* or \*xml\*, where \* is a wildcard. Make sure that other file types, e.g. binary files, have the correct HTTP content type, otherwise they may get corrupted by the URL hardening feature. It does not work for dynamic URLs created by client, for example: JavaScript.



**Note:** You can find more information about Static URL Hardening and Form Hardening under: [Additional Information on Static URL Hardening and Form Hardening](#) on page 494

## Entry URLs (only applicable if Static URL Hardening is enabled)

Specify a URL for static URL hardening:

### Form Hardening

Enable this to protect against web form rewriting. Form hardening saves the original structure of a web form and signs it. Therefore, if the structure of a form has changed when it is submitted the Web Application Protection rejects the request.



**Note:** Form hardening affects all files with a HTTP content type of text/\* or \*xml\*, where \* is a wildcard. Make sure that other file types, e.g. binary files, have the correct HTTP content type, otherwise they may get corrupted by the form hardening feature.



**Note:** You can find more information about static URL hardening and form hardening under: [Additional Information on Static URL Hardening and Form Hardening](#) on page 494

## Anti-Virus

Enable this to protect a web server against viruses.

### Mode

Select a mode from the available options.

- Avira
- Sophos
- Dual Scan

## Direction

Select from the drop-down list whether to scan only uploads or downloads or both.

- Uploads
- Downloads
- Uploads and Downloads

## Block unscannable content

Enable this to block files that cannot be scanned. The reason for that may be, among other things, that files are encrypted or corrupt.

## Limit scan size

Enable this to enter the scan size limit into an additional field. Provide the limitation in megabytes.



**Note:** Please note that the scan size limit refers to the entire upload volume, not to a single file. If, for example, you limit the scan size to 50 MB and make an upload containing multiple files (45 MB, 5 MB and 10 MB), the last file will not be scanned. Thus a virus being in the last file would not be detected due to the limitation.



**Note:** If you do not specify a limitation value at all, the limit scan size will be saved with '0' megabytes, which means the limitation is not active and every uploaded/downloaded file will be scanned.

## Block clients with bad reputation

Enable this to block clients which have a bad reputation according to their classification, based on GeoIPClosed and RBLClosed information. Sophos uses the following classification providers: RBL sources:

- Commtouch IP Reputation (ctipd.org)
- http.dnsbl.sorbs.net

The GeoIP source is Maxmind. The WAF blocks clients that belong to one of the following Maxmind categories:

- A1: Anonymous proxies or VPN services used by clients to hide their IP address or their original geographical location.
- A2: Satellite providers are ISPs that use satellites to provide Internet access to users all over the world, often from high risk countries.

## Skip remote lookups for clients with bad reputation (only applicable if Block clients with bad reputation is enabled)

Enable to use GeoIP-based classification which uses cached information only and is therefore much faster. As reputation lookups include sending requests to remote classification providers, using reputation-based blocking may slow down your system.

## Common Threat Filter

Enable this to protect your web servers from several threats. You can specify the threat filter categories you want to use in the Threat Filter Categories section below. All requests will be checked against the rule sets of the selected categories. Depending on the results, a notice or a warning will be shown in the live log or the request will be blocked directly.

## Rigid Filtering

Enable this to tighten several of the selected rules. This may lead to false positives.

## Skip Filter Rules

Some of the selected threat categories may contain rules that lead to false positives. To avoid false positives induced by a specific rule, add the rule number that you want to skip in this field.

## Protocol Violations

Enforces adherence to the RFC standard specification of the HTTP protocol. Violating these standards usually indicates malicious intent.

#### **Protocol Anomalies**

Searches for common usage patterns. Lack of such patterns often indicates malicious requests. These patterns include, among other things, HTTP headers like ‘Host’ and ‘User-Agent’.

#### **Request Limits**

Enforces reasonable limits on the amount and ranges of request arguments. Overloading request arguments is a typical attack vector.

#### **HTTP Policy**

Narrows down the allowed usage of the HTTP protocol. Web browsers typically use only a limited subset of all possible HTTP options. Disallowing the rarely-used options protects against attackers aiming at these often less well-supported options.

#### **Bad Robots**

Checks for usage patterns characteristic of bots and crawlers. By denying them access, possible vulnerabilities on your web servers are less likely to be discovered.

#### **Generic Attacks**

Searches for attempted command executions common to most attacks. After having breached a webserver, an attacker usually tries to execute commands on the server like expanding privileges or manipulating data stores. By searching for these post-breach execution attempts, attacks can be detected that might otherwise have gone unnoticed, for example because they targeted a vulnerable service by the means of legitimate access.

#### **SQL Injection Attacks**

Checks for embedded SQL commands and escape characters in request arguments. Most attacks on web servers target input fields that can be used to direct embedded SQL commands to the database.

#### **XSS Attacks**

Checks for embedded script tags and code in request arguments. Typical cross-site scripting attacks aim at injecting script code into input fields on a target web server, often in a legitimate way.

#### **Tight Security**

Performs tight security checks on requests, like checking for prohibited path traversal attempts.

#### **Trojans**

Checks for usage patterns characteristic of trojans, thus searching for requests indicating trojan activity. It does not, however, prevent the installation of such trojans as this is covered by the antivirus scanners.

#### **Outbound**

Prevents web servers from leaking information to the client. This includes, among other things, error messages sent by servers which attackers can use to gather sensitive information or detect specific vulnerabilities.

The form contains the following fields:

- Name \*: Text input field.
- Description: Text area.
- Pass Outlook Anywhere: Switch button (OFF).
- Mode \*: Select dropdown menu showing "Please select".
- Cookie Signing: Switch button (OFF).
- Static URL Hardening: Switch button (OFF).
- Form Hardening: Switch button (OFF).
- Anti-Virus: Switch button (OFF).
- Block clients with bad reputation: Switch button (OFF).
- Common Threat Filter: Switch button (OFF).

**Figure 456: Add Application Protection Policy**

3. Click Save.

#### Additional Information on Static URL Hardening and Form Hardening

It is best practice always to enable both static URL hardening and form hardening. These two functions are complementary, especially in the way that they prevent the issues you may have if you enable just one of them:

- Only form hardening is activated: When a webpage contains hyperlinks with appended queries (which is the case with certain CMSs), e.g. `http://example.com/?view=article&id=1`, such page requests are blocked by form hardening because it expects a signature, which is missing.
- Only static URL hardening is activated: When a web browser appends form data to the action URL of the form tag of a web form (which is the case with GET requests), the form data becomes part of the request URL sent to the web server, thereby rendering the URL signature invalid.

Activating both functions helps to solve the problems those issues because if either form hardening or static URL hardening consider a request to be valid, the Web Application Protection accepts the request.

## Authentication Policies

The **Authentication Policies** menu allows you to configure policies for direct authentication.

You can use the Web Application Firewall (WAF) to authenticate users immediately instead of leaving the authentication to the web servers. Via authentication profiles, the reverse authentication can be used to assign specific authentication settings to each site path route.

**Note:** You can also view and manage the WAF status on the **System > Hosts and Services > Services** page.

This page displays all existing web application authentication profiles. For each authentication policy, the list shows:

### Name

Name of the authentication policy.

### Add Authentication Policy

This page describes how to add a web app authentication policy.

1. Go to **Protect > Web Server > Authentication Policies** and click **Add**.
2. Enter a unique **Name** for the authentication profile.
3. Enter a **Description** for the authentication policy.
4. Specify the **Client Authentication** details.

#### Mode

Select how the users should authenticate at the Web Application Firewall.

- **Basic:** Users authenticate with HTTP basic authentication, entering username and password. In this mode, no session cookies will be generated and a dedicated logout is not possible.
 

 **Note:** As the credentials are sent unencrypted in this mode we strongly recommend that you use this mode over HTTPS.
- **Form:** Users will be presented with a form where they have to enter their credentials. In this mode, session cookies will be generated and a dedicated logout is possible. The form template to be used can be selected in the **Web App Auth Template** list. Besides the default form template, the list shows the forms that have been defined on the [Authentication Templates](#) page

#### Basic Prompt (*available only if Basic mode is selected*)

The realm is a unique string that provides additional information on the login page and is used for user orientation.

-  **Note:** These characters are allowed for the **Basic Prompt**: A-Z a-z 0-9 , ; . : - \_ ' + = ) ( & % \$ ! ^ < > | @

#### Web App Auth Template (*available only if Form mode is selected*)

Select the form template that will be presented to the users for authentication. Form templates are defined on the [Authentication Templates](#) page.

#### Users or Groups

Select the users or user groups that should be assigned to this web app authentication profile or create a new one. After assigning this profile to a site path route, these users will have access to the site path with the authentication settings defined in this profile. Typically, this would be a backend user group.

You can create a new user directly from this page or from the **Configure > Authentication > Users** page.

[Registering a New User](#) on page 183

You can create a new group directly from this page or from the **Configure > Authentication > Groups** page.

[Creating a New User Group](#) on page 178

-  **Note:** Sometimes users should be required to use the user principal name notation ‘user@domain’ when entering their credentials, for example when using Exchange servers in combination with Active Directory servers.

5. Specify the **Authentication Forwarding** details.

#### Mode

Select how the Web Application Firewall authenticates against the web servers. The mode has to match the web servers’ authentication settings.

- **Basic:** Authentication works with HTTP basic authentication, providing username and password.
- **None:** There is no authentication between WAF and the web servers. Note that even if your web servers do not support authentication, users will be authenticated via the frontend mode.

#### Username affix (*available only if authentication forwarding mode Basic is selected*)

Select the type of affix for the username and specify a value for it. Affixes are useful when working with domains and email addresses.

- None
- Prefix
- Suffix
- Prefix & Suffix

 **Note:** Prefix and suffix will be added automatically if the user only enters his username. Prefix and suffix will not be added if the user enters them. Example: If the suffix is @testdomain.de and the user only enters the username test.user the suffix @testdomain.de will be added. If the user enters test.user@testdomain.de the suffix will be ignored.

#### **Remove Basic Header (*available only if authentication forwarding mode None is selected*)**

Enable this if you do not want to send the basic header from Sophos XG Firewall to the web server.

#### **6. Specify the User Session details (*available only if client authentication mode Form is selected*).**

##### **Session Timeout**

Enable to set a timeout for the user session, which will confirm the user's credentials by requiring the user to log in again if he does not perform any action.

Default: ON

##### **Limit to (*available only if Session Timeout is selected*)**

Set an interval for the session timeout.

Default: 5 minutes.

##### **Session Lifetime**

Enable to limit the time users may remain logged in, regardless of the activity in the meantime.

Default: ON

##### **Limit to (*available only if Session Lifetime is selected*)**

Set a value for the session lifetime.

Default: 8 hours.

The screenshot shows a configuration interface for adding a web application authentication policy. It includes fields for:

- Name \***: A text input field.
- Description**: A text area.
- Client Authentication** section:
  - Mode**: A dropdown menu set to "Basic".
  - Basic Prompt \***: A text input field.
  - Users or Groups**: A list box containing "Add New Item".
- Authentication Forwarding** section:
  - Mode**: A dropdown menu set to "Basic".
  - Username affix**: A dropdown menu set to "None".

**Figure 457: Add Web App Authentication Policy**

7. Click **Save**.

## Authentication Templates

The **Authentication Templates** menu allows you to upload HTML forms for reverse authentication.

A web application authentication template can be assigned to an authentication profile with frontend mode **Form**. The respective form will be presented when a user tries to access a site path to which the authentication profile is assigned.

This page displays all existing web application authentication templates. For each template, the list shows:

### Name

Name of the template.

### Template

Filename of the template.

### Add Authentication Template

This page describes how to add a web application authentication template.

1. Go to **Protect > Web Server > Authentication Templates** and click **Add**.
2. Specify the following:

#### Name

Enter a unique name for the template.

#### Description

Enter a description for the template.

#### HTML template

Select an HTML template.

#### Images/Stylesheet

Select images, stylesheets, or JavaScript files that are used by the selected template.

3. Click **Upload**.

The screenshot shows a configuration interface for adding a Web App Auth Template. It includes fields for 'Name \*' (with a red asterisk), 'Description', 'HTML template \*' (with a 'Browse...' button and a note 'No file selected.'), 'Images/Stylesheet' (with a 'Browse...' button and a note 'No file selected.'), and an 'Upload' button.

**Figure 458: Add Web App Auth Template**

4. Click Save.

## SlowHTTP Protection

This page describes how to activate SlowHTTP protection and define the keys used for cookie signing and URL hardening.

The **SlowHTTP Protection** page helps to protect against Slow HTTP attacks by setting a timeout for request headers. For more information, see [Sophos Knowledge Base](#).

1. Go to **Protect > Web Server > SlowHTTP Protection**.

2. Specify the **SlowHTTP Protection Settings**:

### Timeout for request headers

Click the toggle switch to activate SlowHTTP Protection.

#### Soft limit

Enter the minimum amount of time to receive a request header.

Default: 10 seconds



**Note:** The hard limit needs to be greater than the soft limit.

#### Hard limit

Enter the maximum amount of time to receive the request header.

Default: 30 seconds

#### Extension rate

Enter the amount of data volume which extends the timeout.

With the extension rate, you can increase the minimal timeout according to the data volume. For example, the soft limit allows at least 10 seconds to receive request headers, the extension rate is 500, and the hard limit is set to 30. If the client now sends data, the soft limit timeout increases 1 second for every 500 bytes received. After 30 seconds the client will be disconnected.

Default: 5000 Bytes

#### Skipped Networks/Hosts

Select or add networks/hosts that should not be affected by SlowHTTP Protection.

Timeout for request headers

Soft limit \*  Second(s)

Hard limit \*  Second(s)

Extension rate \*  Byte(s)

Skipped Networks/Hosts

Add New Item

**Figure 459: SlowHTTP Protection Settings**

3. Click **Apply**.

## Advanced Threat

This chapter describes how to configure the advanced threat features of Sophos XG Firewall.

Advanced threat features are:

- Advanced Threat Protection
- Security Heartbeat

Those features require a valid Network Protection subscription.

### Advanced Threat Protection

This page allows the administrator to configure the Advanced Threat Protection feature.

ATP can help rapidly detect infected or compromised clients inside the network and raise an alert or drop the respective traffic.

The Advanced Threat Protection analyzes network traffic, e.g., DNS requests, HTTP requests, or IP packets in general, coming from and going to all networks. It also incorporates Intrusion Prevention and Antivirus data if the respective features are activated.



**Note:** Advanced Threat Protection module is a subscription module that needs to be subscribed before use.

#### General Settings

##### Enable Advanced Threat Protection

By default Advanced Threat Protection is disabled. To enable Advanced Threat Protection, click on the slider. This will make several setting fields editable.

##### Logging (*available only if Enable Advanced Threat Protection is enabled*)

Logging is enabled. You can change the log setting by clicking **Change log settings** or by navigating to the **Configure > System Services > Log Settings** page and clicking **Add Syslog Server**.

#### Policy

Select the security policy that the Advanced Threat Protection system should use if a threat has been detected.

Available Options:

- **Log and Drop** - The data packet will be dropped and logged.
- **Log Only** - The data packet will be logged.

### Network/Host Exceptions

Add or select the source networks or hosts that should be exempt from being scanned for threats by Advanced Threat Protection. How to add an IP host is explained on the **System > Hosts and Services > IP Host** page.

### Threat Exceptions

Add destination IP addresses or domain names that you want to skip from being scanned for threats by Advanced Threat Protection.

**Caution:** Be careful with specifying exceptions. By excluding sources or destinations you may expose your network to severe risks.

**Figure 460: Advance Threat Protection**

The screenshot shows the 'Advanced Threat Protection' configuration page. At the top, there is a toggle switch labeled 'ON' for 'Enable Advanced Threat Protection'. Below it, under 'Logging', there is an 'Enable' checkbox and a link to 'Change log settings'. A dropdown menu for 'Policy \*' is set to 'Log and Drop'. Under 'Network / Host Exceptions', there is a large empty list area with a button labeled 'Add New Item'. Under 'Threat Exceptions', there is another large empty list area with a search bar labeled 'Search / Add' and a plus sign icon.

### Sandstorm Activity

Activity records provide basic information such as the date and time on which files were sent to Sandstorm. They also indicate analysis and release status. Use the links provided to view report details and release files.

To filter the list, click the Filter button (  ) and specify criteria. For example, you can filter on a date range or file type.

To view details of a Sandstorm analysis, click **Show report**. Reports contain the following:

- Download details, for example, the source and download time
- File details, for example, the file name and type
- Result of the Sandstorm analysis
- Description of the potential threats contained by the file
- A list of all users who have downloaded the file

To release a file, click **Release Now**. When you release a file, users can download it immediately. Only files that are currently being analyzed or that have been returned with error status are eligible for release.

Sandstorm continues to analyze the file even if you release it.

 **CAUTION:** Releasing an item before the analysis is complete may result in the downloading of malicious content.

**Date**

Date and time on which the file was sent to Sandstorm.

**Recipient**

IP address and user name associated with the download.

**Source**

Domain or IP address from which the user downloaded the file and the download type (web or email).

**File Type**

Type of file downloaded.

**Status**

Status of the analysis.

**Manage**

View release status and release files.

## Sandstorm Settings

Use these settings to specify cloud location and files to exclude from Sandstorm analysis.

**Cloud Location**

Files to be analyzed by Sandstorm are transmitted using a secure SSL connection to a data center in the cloud. Data centers are located in the United States and Europe. By default, Sandstorm selects the closer data center according to the location of the device. You can override the default behavior by selecting a data center.



**Note:** Changing data centers may affect any analysis that is currently in progress.

**Exclude File Types**

A file type is a classification that is determined by file extension and MIME header. Click **Add New Item** and select file types that you do not want to send to Sandstorm for analysis. Exclusions apply to web and email traffic.



**Note:** Any archive that includes a file of the selected type will also be excluded, regardless of what other types of files that archive may contain.



**Note:** Although you can add an exclusion for any type of file, many file types that are considered safe (for example, images) will never be sent to Sandstorm. Only risky file types that Sandstorm can detonate and analyze will be sent.

**Related concepts**

[File Types](#) on page 397

A file type is a classification that is determined by file extension and MIME header. You can include file types in web policies to control access to files that match the specified criteria. The default file types contain some common criteria and you can create additional types.

## Synchronized Security

The Synchronized Security menu allows you to configure Security Heartbeat to share health information and the Synchronized Application Control.

Security Heartbeat connects cryptographically secured endpoints and Sophos XG Firewall via Sophos Central. This allows to exchange information between endpoint devices and Sophos XG Firewall. This information gives a comprehensive overview of the network security. The administrator is able to define policies for network access based on the health status of the endpoint. The Security Heartbeat widget on the Control Center page provides the health status of all endpoint devices.



**Note:** If traffic will be routed through a VPN connection before the heartbeat connection has been established, the heartbeat traffic will also be routed through the VPN tunnel and thus, the firewall cannot

see this heartbeat traffic and marks the endpoint as missing. When the endpoint is in missing state, all traffic through the firewall from this endpoint will be blocked.



**Note:** A missing heartbeat will not be detected by Sophos XG Firewall if the endpoint is located behind an intermediate router. This does not lead to false results and the endpoint will still share the health status. **Security Heartbeat** is not supported if the router is a NAT gateway, i.e. the endpoints do not share the health status with Sophos XG Firewall.

Endpoint devices and users need to authenticate via Sophos Central to connect to Sophos XG Firewall. The authentication works via a client which is available on Sophos Central and must be installed on the endpoint device. Once the installation is completed, the endpoint uses the **Sophos Endpoint Security and Control** which is an integrated suite of security software, for example, antivirus, behavior monitoring and live protection. **Sophos Endpoint Security and Control** ensures that the endpoint device belongs to the system and has the permission to access the network.



**Note:** For more information and documentation about **Sophos Endpoint Security and Control** visit the [Sophos Website](#).

In regular intervals, the endpoint sends a heartbeat signal to Sophos XG Firewall to show that it is alive. Furthermore, the endpoint also informs the Sophos XG Firewall about potential threats. If **Sophos Endpoint Security and Control** detects any threats, the endpoint sends this information to Sophos XG Firewall which declares the endpoints health status. Depending on the user policy which defines the permission of the different health status, the endpoint may not be able to connect to networks, zones or services.



**Note:** You can enable **Security Heartbeat** and set the **Minimum Heartbeat Permitted** in the **User / Network Rule** which is managed on the **Firewall > Add User / Network Rule** page in the **Security Heartbeat** section.



**Note:** Please find a description of the endpoints' health status colors on the **Health Status** page.



**Note:** Sophos XG Firewall does not support **Security Heartbeat** with bonded interfaces on MAC endpoints.

## Related concepts

[Control Center](#) on page 11

[User / Network Rule](#) on page 306

User/Network Rule is used to define access rights and protection to the network objects/hosts. In a nutshell, if you want to control traffic by source, service, destination, zone, then use a **Network Rule**. Additionally, the administrator has the option to attach user identity to a rule in order to customize access of assorted hosts/servers. Such an identity based rule is considered a **User Rule**.

## Security Heartbeat Global Configuration

This page describes how to log in with your Sophos Central account and enable Security Heartbeat.

To use Security Heartbeat you need to register with your Sophos Central account. If you do not have an account you can create a new one (see the steps below).



**Note:** For more information about Sophos Central, see: <https://www.sophos.com/en-us/lp/sophos-central.aspx>.

1. Go to **Protect > Synchronized Security**.
2. Specify the Sophos Central login details.



**Note:** You can also create a Sophos Central account by clicking **Create Sophos Central Account**.

3. Click **Register**.

You are registered with your Sophos Central ID to the Sophos XG Firewall. Security Heartbeat is enabled.

4. Add zones to the **Missing Heartbeat Zones** field.

Missing heartbeats will be detected only in these zones.



**Note:** If a zone is blocked by a policy but no zone is added here, the Security Heartbeat widget in the Control Center shows "Missing".

## 5. Click **Apply**.

If you disable Security Heartbeat you are still registered with your Sophos Central account. To clear your registration from Sophos XG Firewall, click **Clear Registration**.

### **Activate Synchronized Application Control**

Ensure that you are registered for Security Heartbeat (see [Security Heartbeat Global Configuration](#) on page 502).

1. Go to **Synchronized Security**.
2. Enable **Synchronized Application Control**.
3. Click **Apply**.

Synchronized App Control is now active and you can see newly detected applications on **Applications > Synchronized Application Control**.

---

## Appendix A - Logs

---

Device provides extensive logging capabilities for traffic, system, and network protection functions. Detailed log information and reports provide historical as well as current analysis of network activity to help identify security issues and reduce network misuse and abuse.

Device provides following logs:

- System Logs
- Web Filter Logs
- Application Filter Logs
- Malware Logs
- Email Logs
- Firewall Logs
- IPS Logs
- Authentication Logs
- Admin Logs
- Sandstorm Logs
- Web Server Protection Logs
- Advanced Threat Protection Logs
- Security Heartbeat Logs
- Web Content Policy Logs

To view logs for all modules, go to [Log Viewer](#) page.

---

## Log Viewer

---

Use **Log Viewer** to view the logs for modules like System, Web filter, Application Filter, Malware, Email, Firewall, IPS, Authentication, Admin, Sandstorm, Web Server Protection, Advanced Threat Protection, Security Heartbeat and Web Content Policy. This page gives consolidated information about all the events logged by your device.

You can also open multiple live packet capture windows with different filters from this page. To view them, you need to enable **Packet Capture** from **Monitor & Analyze > Diagnostics > Packet Capture**. It is recommended to enable **Wrap Capture Buffer Once Full** on [Configure Capture Filter](#) page to continue capturing packets after the buffer is full.

Click **Open PCAP** link under **Live PCAP** column to view packet capture in a new window. It will display the packet captures that are automatically filtered based on the values of the currently selected packet. Click **Display Filter** in

the packet capture window to modify the filters. You cannot open packet capture window for the following modules: **System** and **Admin**.

Using this page, you can:

- Refresh: Click the **Refresh** button  to refresh logs.
- Pause: Click the **Pause** button  to pause live logs. Live logs will pause when you scroll down the Log Viewer screen.
- Export: Click the **Export** button  to export log details in MS Excel format. The excel sheet contains all the logs available in the Log Viewer grid.
- View logs using any of the two options:
  - Click the **Standard View** button  to view module-wise log details. By default, the logs are displayed for Firewall module.

Instead of switching to **Detailed View**, move the pointer over the module icon to view detailed logs. For example, for Firewall module, move the pointer over  icon to view detailed logs.

 **Note:** At a time you can select only one module.

- Click the **Detailed View** button  to view comprehensive log lines.
-  **Note:** By default, all modules are selected. Select or deselect the modules from the drop-down list.
- Search: Enter text to be searched. Result will be highlighted in the records.

 **Note:** Last search is retained when you switch views.

- Filter:
  - Click **Add Filter**, select the **Field**, select the **condition** and enter the **Value** for filter criteria.
  - Click the **Quick Filter** button  next to **Add Filter** to view logs for the time interval that you specify.
- View logs for all 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.
  - *Sandstorm* - Sandstorm logs provide information about the enhanced protection provided against advanced and targeted attacks.
  - *Web Server Protection* – Web Server Protection 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.
  - *Web Content Policy* - Web Content Policy provide information about content filter matches and its associated details.

## View List of System Events

### Time

Time when the event occurred.

### Log Comp

Displays the log components of the system event.

Log component types – HTTP, HA, central management, IPSec, L2TP, PPTP, SSL VPN, Device, DHCP Server, Interface, Gateway, DDNS, WebCat, IPS, anti-virus, quarantine, WLAN, HTTPS, guest user, protected application server, CTA, PPPoE, wireless protection, RED, ATP, SSL VPN Client, IPSec client, authentication clients, RED firmware, AP firmware and Up2Date.

### Status

Successful: Displays event is successful.

Failed: Displays event is failed.

### Username

Username of the user.

### Message

Message for the type of system event.

### Message ID

Message ID of the message.

	Time	Log Comp	Status	Username	Message	Message ID
 SYSTEM	2017-09-06 12:02:42	Up2Date	Failed		Failed to check for updates	18029
 SYSTEM	2017-09-06 10:02:58	Appliance			Appliance started successfully.	17816
 SYSTEM	2017-09-06 10:02:50	Interface			Interface PortB is Up	17813
 SYSTEM	2017-09-06 10:02:50	Interface			Interface PortB is Down	17813
 SYSTEM	2017-09-06 10:02:47	Wireless Protection			new firmware detected for RED15w_1	17998

**Figure 461: System Log**

## View List of Web Filter Events

Logs are displayed only if the Web Protection module is subscribed.

### Time

Time when the event occurred.

### Action

Allowed: Displays websites allowed by the device.

Denied: Displays websites blocked by the device.

### Username

Username of the user that accessed the URL.

### Source IP

Source IP address (IPv4/IPv6).

### Destination IP

Destination IP address (IPv4/IPv6).

### Category

**Web Category** under which the URL is categorized by the device.

### URL

URL accessed.

### Bytes Sent

Number of bytes sent.

### Message ID

Message ID of the message.

### Policy ID

Policy ID applicable to the message.

### Transaction ID

Indicates the transaction ID of the AV scan.

### Live PCAP

Click **Open PCAP** link to view packet capture in a new window based on Source IP, Policy ID and Username.

Time	Action	Username	Source IP	Destination IP	Category	URL	Bytes Sent	Referrer	Message ID	Policy ID	Transaction ID	Live PCAP
13.09.2017 - 18:46	Allowed		10.8.142.3	10.8.142.181	Information Technology	http://ta-web-static.qa.astaro.de/ta-testfiles/old_sav/vdl/vdl176.vdb	267		18001	2	ec403b23-a612-4f10-a618-ec14c03fb5ca	<a href="#">Open PCAP</a>
13.09.2017 - 18:46	Allowed		10.8.142.3	10.8.142.181	Information Technology	http://ta-web-static.qa.astaro.de/ta-testfiles/old_sav/vdl/vdlH2.vdb	268		18001	2	9225e1aa-55ab-43cd-8948-d357c8c82f1	<a href="#">Open PCAP</a>
13.09.2017 - 18:46	Allowed		10.8.142.3	10.8.142.181	Information Technology	http://ta-web-static.qa.astaro.de/ta-testfiles/old_sav/vdl/vdlH9.vdb	265		18001	2	f38394bb-1caa-46bb-aa33-bd1ac65bea20	<a href="#">Open PCAP</a>
13.09.2017 - 18:46	Allowed		10.8.142.3	10.8.142.181	Information Technology	http://ta-web-static.qa.astaro.de/ta-testfiles/old_sav/vdl/vdl108.vdb	267		18001	2	850c385f-4672-4c4b-b418-85efcdc25abc	<a href="#">Open PCAP</a>

**Figure 462: Web Filter Log Viewer**

## View List of Application Filter Events

**Logs are displayed only if the Web Protection module is subscribed.**

### Time

Time when event occurred.

### Action

Denied.

### Username

Username of the user that accessed the application.

### Source IP

Source IP address (IPv4/IPv6).

### Destination IP

Destination IP address (IPv4/IPv6).

### Application Category

Category under which the application is categorized.

### Application

Name of the application denied.

### Message ID

Message ID of the message.

### Policy ID

Policy ID applicable to the message.

### Live PCAP

Click **Open PCAP** link to view packet capture in a new window based on Source IP, Policy ID and Username.

	Time	Action	Username	Source IP	Destination IP	Application Category	Application	Message ID	Policy ID	Live PCAP
Application Filter	11.09.2017 - 14:05	Denied	10.198.235.172	10.198.235.172	91.190.219.41	P2P	Torrent Clients P2P	17051	1	<a href="#">Open PCAP</a>
Application Filter	11.09.2017 - 14:04	Denied	10.198.232.160	10.198.232.160	91.190.218.55	P2P	Torrent Clients P2P	17051	1	<a href="#">Open PCAP</a>
Application Filter	11.09.2017 - 14:04	Denied	10.198.237.31	10.198.237.31	91.190.218.59	P2P	Torrent Clients P2P	17051	2	<a href="#">Open PCAP</a>
Application Filter	11.09.2017 - 14:04	Denied	10.198.235.172	10.198.235.172	91.190.218.56	P2P	Torrent Clients P2P	17051	1	<a href="#">Open PCAP</a>

**Figure 463: Application Filter Log Viewer**

## View List of Malware Events

**HTTP, HTTPS, and FTP logs are displayed only if the Web Protection module is subscribed.**

**POP, POP3, IMAP, IMAPS, SMTP and SMTPS logs are displayed only if Email Protection module is subscribed.**

### Time

Time when the event occurred.

### Protocol

Application protocol or firewall component that detected the malware.

### Username

Username of the user on whose system, virus was detected.

### Source IP

IP address and port from which the connection originated (client-side).

### Destination IP

IP address and port to which the connection is directed (server-side).

### Virus

Name of the malware identified by the scan engine.

### Message

Protocol-specific information about the event.

### Message ID

Message ID of the message.

### Live PCAP

Click **Open PCAP** link to view packet capture in a new window based on Source IP and Username.

**Figure 464: Malware Log Viewer**

	Time	Protocol	Username	Source IP	Destination IP	Virus	Message	Message ID	Live PCAP
Malware	13.09.2017 - 18:45	HTTP		10.99.117.150	10.99.113.146	EICAR-AV-Test		08001	<a href="#">Open PCAP</a>
Malware	13.09.2017 - 18:45	HTTP		10.8.142.3	10.8.142.181	Troj/Agent-AMOA,Mal/DrodCab-A	08001		<a href="#">Open PCAP</a>
Malware	13.09.2017 - 18:44	HTTP		10.8.142.3	10.8.142.181	Troj/DocDI-EDF		08001	<a href="#">Open PCAP</a>
Malware	13.09.2017 - 18:44	HTTP		10.8.142.3	10.8.142.181	Troj/DocDI-EDF		08001	<a href="#">Open PCAP</a>

## View List of Email Events

**Logs are displayed only if the Email Protection module is subscribed.**

### Time

Time when the event occurred.

**Protocol**

Displays the protocols of the email events.

Types of protocols: SMTP, SMTPTS, POP, POPS, IMAP and IMAPS.

**Email Action**

Displays action taken against any email events.

Actions: Reject, Drop, Accept, Change Recipient, Prefix Subject, Tmp Reject and Accept with SPX.

**Username**

Username of the user on whose system, spam was detected.

**Source IP**

Source IP address (IPv4/IPv6).

**Destination IP**

Destination IP address (IPv4/IPv6).

**Email Sender**

Email address of the sender.

**Email Receiver**

Email address of the recipient.

**Email Subject**

Subject of the email.

**Message**

Message related to action taken by the device for the email event.

**Message ID**

Message ID of the message.

**Live PCAP**

Click **Open PCAP** link to view packet capture in a new window based on Source IP and Username.

**Figure 465: Email Log Viewer**

Time	Protocol	Email Action	Username	Source IP	Destination IP	Email Sender	Email Receiver	Email Subject	Message	Message ID	Live PCAP
2017-09-22 17:36:41	SMTP			10.198.47.206	10.198.241.48	john.smith@sophos.com	alice.kim@sophos.com	*****Non-disclosed subject		13011	<a href="#">Open PCAP</a>
2017-09-22 17:36:41	SMTP			10.198.47.206	10.198.241.48	john.smith@sophos.com	alice.kim@sophos.com	*****Non-disclosed subject		13009	<a href="#">Open PCAP</a>
2017-09-22 17:36:59	SMTP			10.198.47.206	10.198.241.48	john.smith@sophos.com	alice.kim@sophos.com	*****Non-disclosed subject		13011	<a href="#">Open PCAP</a>
2017-09-22 17:36:59	SMTP			10.198.47.206	10.198.241.48	john.smith@sophos.com	alice.kim@sophos.com	*****Non-disclosed subject		13003	<a href="#">Open PCAP</a>

**View List of Firewall Events****Time**

Time when the event occurred.

**Log Comp**

Displays the log components of the firewall events.

Examples: firewall rule, invalid traffic, local ACL, DoS attack, ICMP redirection, source routed, fragmented traffic, MAC filter, IPMAC filter, IP spoof , protected application server heartbeat and ICMP error message.

**Action**

Allowed: Permits the traffic.

Denied: Restrict the traffic.

**Username**

Username of the user on which the firewall rule is applied.

**Firewall Rule**

Firewall rule ID.

**In Interface**

Interface through which the traffic is coming in.

**Out Interface**

Interface through which the traffic is going out.

**Source IP**

Source IP address (IPv4/IPv6).

**Destination IP**

Destination IP address (IPv4/IPv6).

**Rule Type**

Type of firewall rule.

**Message ID**

Message ID of the message.

**Live PCAP**

Click **Open PCAP** link to view packet capture in a new window based on Source IP, Firewall Rule ID and Username.

**Message**

Message for the type of firewall event.

Time	Log Comp	Action	Username	Firewall Rule	In Interface	Out Interface	Source IP	Destination IP	Rule Type	Message ID	Live PCAP	Message
2017-09-28 03:46:30		Invalid Traffic	Denied	0			103.5198.210	10.198.46.27	0	01001	<a href="#">Open PCAP</a>	Could not associate packet to any connection
2017-09-28 03:46:30		Invalid Traffic	Denied	0			103.5198.210	10.198.46.27	0	01001	<a href="#">Open PCAP</a>	Could not associate packet to any connection
2017-09-28 03:46:29		Invalid Traffic	Denied	0			103.243.111.210	10.198.46.27	0	01001	<a href="#">Open PCAP</a>	Could not associate packet to any connection
2017-09-28 03:46:28		Invalid Traffic	Denied	0			103.5198.210	10.198.46.27	0	01001	<a href="#">Open PCAP</a>	Could not associate packet to any connection

**Figure 466: Firewall Log Viewer**

**View List of IPS Events**

Logs are displayed only if the Network Protection module is subscribed.

**Time**

Time when the event occurred.

**Log Comp**

Displays the log components of IPS events.

Types of log components: anomaly and signatures.

**Action**

Detect: Intrusion attempts detected by the device.

Drop: Intrusion attempts dropped by the device.

**Username**

Username of the user that triggered the signature.

**Source IP**

Source IP address (IPv4/IPv6).

**Destination IP**

Destination IP address (IPv4/IPv6).

#### **Signature ID**

Signature ID of the signature.

#### **Signature Name**

Name for the detected signature.

#### **Category**

Category of the signature.

#### **Platform**

Platform of the signature.

#### **Victim**

Victim of the signature.

#### **Firewall Rule**

Firewall rule applied.

#### **Message ID**

Message ID of the message.

#### **Live PCAP**

Click **Open PCAP** link to view packet capture in a new window based on Source IP and Username.

**Figure 467: IPS Log Viewer**

Time	Log Comp	Action	Username	Source IP	Destination IP	Signature ID
2015-11-02 14:53:25	Signatures	Detect	dp	10.198.233.55 :ICMP(768)	10.198.47.102 :ICMP(256)	399
2015-11-02 14:53:16	Signatures	Detect	dp	10.198.233.55 :ICMP(768)	10.198.47.102 :ICMP(256)	399
2015-11-02 14:53:16	Signatures	Detect	dp	10.198.233.55 :ICMP(768)	10.198.47.102 :ICMP(256)	399
2015-11-02 14:53:05	Signatures	Detect	dp	4.2.2.2 :ICMP(0)	10.198.47.102 :ICMP(0)	408
2015-11-02 14:53:05	Signatures	Detect	dp	10.198.47.102 :ICMP(2048)	4.2.2.2 :ICMP(0)	384

#### **View List of Authentication Events**

##### **Time**

Date and time when the event occurred.

##### **Log Comp**

Displays the log components of the authentication events.

Type of log components: external authentication, firewall authentication, VPN authentication, SSL VPN authentication, My Account authentication, Dial-In authentication and NTLM authentication.

##### **Status**

Successful: Displays the successful events.

Failed: Displays the failed events.

##### **Username**

Username of the user.

**Source IP**

IP address of the user.

**Auth Client**

Authentication client that is used for authentication.

**Auth Mechanism**

Type of authentication mechanism: local or external server (AD, LDAP or RADIUS).

**Signature Name**

Signature name for the type of authentication event.

**Message ID**

Message ID of the message.

**Live PCAP**

Click **Open PCAP** link to view packet capture in a new window based on Source IP and Username.

	Time	Log Comp	Status	Username	Source IP	Auth Client	Auth Mechanism	Signature Name	Message ID	Live PCAP
Authentication	2017-09-22 18:20:11	Web Application Firewall	Failed	admin	10.198.235.254	WAF	Local	User admin failed to login to WAF through Local authentication mechanism because of wrong credentials	17708	<a href="#">Open PCAP</a>
Authentication	2017-09-22 18:18:47	Web Application Firewall	Failed	admin	10.198.235.254	WAF	Local	User admin failed to login to WAF through Local authentication mechanism because of wrong credentials	17708	<a href="#">Open PCAP</a>
Authentication	2017-09-22 18:12:37	Web Application Firewall	Failed	admin	10.198.235.254	WAF	Local	User admin failed to login to WAF through Local authentication mechanism because of wrong credentials	17708	<a href="#">Open PCAP</a>
Authentication	2017-09-22 18:07:49	Web Application Firewall	Failed	admin	10.198.235.254	WAF	Local	User admin failed to login to WAF through Local authentication mechanism because of wrong credentials	17708	<a href="#">Open PCAP</a>

**Figure 468: Authentication Log Viewer**

**View List of Admin Events****Time**

Time when the event occurred.

**Log Comp**

Displays type of log components of admin events. Types of log components: GUI, CLI, API and central management.

**Status**

Successful: Displays the successful events.

Failed: Displays the failed events.

**Username**

Username of the admin user.

**Source IP**

IP address of the admin user.

**Signature Name**

Signature name for the type of admin event.

**Message ID**

Message ID of the message.

	Time	Log Comp	Status	Username	Source IP	Signature Name	Message ID
Admin	2017-09-28 03:48:36	GUI	Successful	admin	10.198.46.31	Administrator 'admin' logged in successfully to Web Admin Console.	17507
Admin	2017-09-28 03:31:58	GUI	Successful	admin	10.198.47.73	Administrator 'admin' logged in successfully to Web Admin Console.	17507
Admin	2017-09-28 02:55:50	CLI	Successful	admin	10.198.46.31	User 'admin' logged in successfully from '10.198.46.31' using telnet.	17507
Admin	2017-09-28 02:55:14	CLI	Successful	admin	127.0.0.1	Appliance Access was enabled by 'admin' from '127.0.0.1' using 'CLI'	17505

**Figure 469: Admin Log Viewer**

## View List of Web Server Protection (WAF) Events

Logs are displayed only if Web Server Protection module is subscribed.

### Time

Time when the event occurred.

### Server

Displays the name of the web server.

### Source IP/Name

Source IP address or name.

### URL

URL accessed.

### Reason

Reason for the action taken on any web application.

### Message

Message for the WAF event.

### Status Code

Status code of the action taken on the web application.

### Bytes Received

Displays the information of bytes received by the device.

### Bytes Transmitted

Displays the information of bytes transmitted by the device.

### Message ID

Message ID of the message.

### Policy ID

Policy ID applicable to the WAF event.

### Live PCAP

Click **Open PCAP** link to view packet capture in a new window based on Source IP and Policy ID.

Time	Server	Source IP/Name	URL	Reason	Message	Status Code	Bytes Received	Bytes Transmitted	Message ID	Policy ID	Live PCAP
2017-09-22 18:42:48	www.sophos.com:8989	10.198.235.254	/Form with passthrough_cmlwpitggjwmxrh/company_logo.png	-	-	365	4015	17071	3	<a href="#">Open PCAP</a>	
2017-09-22 18:42:48	www.sophos.com:8989	10.198.235.254	/Form with passthrough_cmlwpitggjwmxrh/default_stylesheet.css	-	-	386	1678	17071	3	<a href="#">Open PCAP</a>	
2017-09-22 18:42:47	www.sophos.com:8989	10.198.235.254	/_cmlwpitggjwmxrh_form	-	-	352	1388	17071	3	<a href="#">Open PCAP</a>	
2017-09-22 18:42:47	www.sophos.com:8989	10.198.235.254	/	-	-	328	532	17071	0	<a href="#">Open PCAP</a>	
2017-09-22 18:34:38	10.198.233.48:8989	10.198.235.254	/	-	-	365	501	17071	0	<a href="#">Open PCAP</a>	

**Figure 470: WAF Log Viewer**

## View List of Advanced Threat Protection Events

Logs are displayed only if the Network Protection module is subscribed.

**Time**

Time when the event occurred.

**Host (Source IP)**

IP address of the host from where the threat derives.

**Username**

Username of the user.

**Destination IP**

Destination IP address (IPv4/IPv6).

**Threat**

Name of the threat detected by the device.

**Threat URL/IP**

URL/IP of the threat detected.

**Origin**

Displays the type of source from where the threat comes (Firewall, DNS, IPS, web).

**Action**

Action taken on the detection of the threat (log only, log and drop).

**Message ID**

Message ID of the message.

**Login User**

Name of the login user.

**Process User**

Name of the process user.

**Executable**

Name of executable files possibly infected with threats.

**Live PCAP**

Click **Open PCAP** link to view packet capture in a new window based on Source IP and User.

Time	Host(Source IP)	User	Destination IP	Threat	Threat URL/IP	Origin	Action
2015-11-02 14:55:02	10.198.47.102	dp	46.165.206.253	C2/Generic-A	46.165.206.253	Firewall	Log
2015-11-02 14:55:02	10.198.47.102	dp	46.165.206.253	C2/Generic-A	46.165.206.253	Firewall	Log
2015-11-02 14:55:01	10.198.47.102	dp	178.89.159.37	C2/Generic-A	178.89.159.37	Firewall	Log
2015-11-02 14:55:01	10.198.47.102	dp	178.89.159.37	C2/Generic-A	178.89.159.37	Firewall	Log

**Figure 471: ATP Log Viewer**

**View List of Security Heartbeat Events****Time**

Time when the event occurred.

**Endpoint Name**

Name of the endpoint.

**Endpoint IP**

IP address of the endpoint.

**Endpoint Health**

Status of endpoint health (red, yellow, green).

**Message ID**

Message ID of the message.

**Live PCAP**

Click **Open PCAP** link to view packet capture in a new window based on Endpoint IP.

Time	Endpoint Name	Endpoint IP	Endpoint Health	Message ID
2015-11-02 15:13:13	W7PRO64XEV	10.198.47.101	Red	18013
2015-11-02 15:11:32	W7PRO64XEV	10.198.47.101	Green	18013

**Figure 472: Security Heartbeat Log Viewer**

## Log ID Structure

---

Log is identified by Log ID. Log ID is a unique 12 characters code c1c2c3c4c5c6c7c8c9c10c11c12

Where:

c1c2 - Log Type ID

c3c4 - Log Component ID

c5c6 - Log Sub Type ID

c7 - Priority

c8c9c10c11c12 - Message ID

For example, if the Log ID is 010101600001.

c1c2 – 01

c3c4 – 01

c5c6 – 01

c7 - 6

c8c9c10c11c12 - 00001

Hence, from the Log ID, we derive:

*Log Type* (01) = Firewall

*Log Component* (01) = Firewall Rule

*Log Sub-type* (01) = Allowed

Message (00001) = Firewall Traffic Allowed (to be seen under appropriate type of logs. Here, since Log Type is Firewall, Message is found under Firewall Logs)

## Log Type

Log Type identifies the type of log.

<b>log_type</b>
Security Policy
IPS
Anti-Virus
Anti Spam
Content Filtering
Event
WAF
ATP
EATP
Wireless Protection
Heartbeat
System Health
Sandstorm

## Log Component

Log Component identifies the component of the log.

<b>log_component</b>
Firewall Rule
Invalid Traffic
Appliance Access
DoS Attacks
ICMP Redirection
Source Routed
Anomaly
Signatures
HTTP
FTP
SMTP
POP3
IMAP4
Fragmented Traffic
Invalid Fragmented Traffic
HA
Foreign Host
IPMAC Filter

log_component
IP Spoof
GUI
CLI
LCD
CCC
IM
IPsec
L2TP
PPTP
SSL VPN
Firewall Authentication
VPN Authentication
SSL VPN Authentication
My Account Authentication
Appliance
DHCP Server
Interface
Gateway
DDNS
WebCat
IPS
AV
Dial-In Authentication
Dial-In
Quarantine
Application Filter
Landing Page
WLAN
ARP Flood
HTTPS
Guest User
WAF
Virtual Host
CTA

<b>log_component</b>
NTLM
Appliances Deactivated
PPPoE
External Authentication
API
ICAP
SMTPS
Wireless Controller
POPS
IMAPS
Firewall
DNS
Web Proxy
Heartbeat
End Point
RED
ATP
SSL VPN Client
IPsec Client
Authentication Client
RED Firmware
AP Firmware
up2date
CPU
Memory
Disk
Live User
Missing Heartbeat
Enhanced app control
ICMP related packets
Mail proxy

## Log Subtype and Module Icons

<b>log_subtype</b>	<b>Color</b>
Allowed	Green
Denied	Red
Detect	Orange
Drop	Red
Clean	Green
Virus	Red
Spam	Red
Probable Spam	Blue
Admin	Blue
Authentication	Blue
System	Blue
OB Clean	Blue
OB Spam	Blue
OB Probable Spam	Blue
No Modification	Blue
Modified Headers	Blue
Modified Body	Blue
4xx Error	Red
5xx Error	Red
Alert	Orange
DLP	Blue
SPX	Blue
DOS	Blue
Override	Blue
Information	Green
Usage	Blue
Warned	Orange
Pending	Blue

**Table 7: Module Icons**

<b>Module Name</b>	<b>Icon and Color</b>
Web Filter	 (Green/Red/Orange)

Module Name	Icon and Color
Application Filter	 (Green)  (Red)  (Orange)
Firewall	 (Green)  (Red)  (Orange)
IPS	 ( Red)
System	 (Green/Red)
Admin	 (Green/Red)
Authentication	 (Green/Red)
Web Server Protection (WAF)	 (Green/Red)
Email	 (Red)

## Common Fields for all Logs

---

Data Fields	Type	Description
device		
date	date	Date (yyyy-mm-dd) when the event occurred
time	time	Time (hh:mm:ss) when the event occurred
message_id	integer	Message ID of the message.
log_id	string	Unique 12 characters code (c1c2c3c4c5c6c7c8c9c10c11) e.g. 0101011, 0102011  c1c2 - Log Type e.g. 01 for firewall log  c3c4 - Log Component i.e. firewall/local ACL/ DoS Attack etc.  c5c6 - Log Sub Type i.e. allow/violation  c7 - Priority e.g. 0 for Emergency  c8c9c10c11 - Message ID e.g. 00001 for traffic allowed by firewall
		Refer <a href="#">Log ID Structure</a>

Data Fields	Type	Description
log_type	string	Type of event e.g. firewall event Refer <a href="#">Log Type</a>
log_component	string	Component responsible for logging e.g. Firewall rule Refer <a href="#">Log Component</a> .
log_subtype	string	Sub type of event Refer <a href="#">Log Sub-type</a> .

## System Logs

Log Component	Message ID	Message
HA	60012	Appliance becomes standalone
	60013	Appliance goes in fault
	60014	Appliance becomes auxiliary
	60015	Appliance becomes primary
	60016	Appliance becomes standalone at appliance start-up
	60017	Appliance goes in fault at appliance start-up
	60018	Appliance becomes auxiliary at appliance start-up
	60019	Appliance becomes primary at appliance start-up
	17838	HA was disabled
DHCP Server	60020	DHCP lease renew
	60021	DHCP lease release
	60022	DHCP lease expired
Appliance	17807	CPU usage exceeded the threshold
	17808	Physical memory usage exceeded the threshold
	17809	SWAP memory usage exceeded the threshold
	17810	Config disk usage exceeded the threshold
	17811	Signature disk usage exceeded the threshold
	17812	Reports disk usage reached the higher threshold
	17816	Appliance started successfully
	17904	Reserved for OPCODE failure snmp trap (logs will be added later)
	17905	Reserved for service failure snmp trap (logs will be added later)
	17923	Scheduled backup was successfully taken (Information)
	17924	Failed to send scheduled backup
	17931	Fan speed has decreased below the desired level
	17932	Temperature has increased above the desired level

	17933	Report disk usage reached lower than the lower threshold
	17934	Report disk usage exceeded the lower threshold
	17941	The audit subsystem has successfully shut down.
	17942	Failed to send certificate passphrase .
	17943	Connectivity to ConnectWise server has been lost.
	17944	Failed to send test mail : <Reason>
Interface	17813	Interface up/interface down
Gateway	17814	Gateway alive/gateway dead
	18036	up/down gateway detail to SFM
DDNS	17815	DDNS update successful/failed
WebCat	17817	WebCat database upgraded from <old version> to <new version>
	17920	WebCat database upgrade failed
AV	17819	AV definitions upgraded from <old version> to <new version>
	17922	AV definitions upgrade failed
IPS	17921	IPS signatures upgrade failed
Interface	17820	Primary link down/up and link failover/fallback to backup/primary link
Dial-in	17821	Dial-in client connected
	17822	Dial-in client disconnected
Quarantine	17823	Quarantined email could not be released because <reason>
SSL VPN	17824	SSL VPN connection (Tunnel Access) established
	17825	SSL VPN connection (Tunnel Access) terminated
	17826	SSL VPN connection (Web Access) established
	17827	SSL VPN connection (Web Access) terminated
	17828	SSL VPN connection (Application Access) established
	17829	SSL VPN connection (Application Access) terminated
	17830	SSL VPN resource access allowed
	17831	SSL VPN resource access denied
	17936	User certificate <certificate_name> was created for user <username>
	17937	All user certificates deleted
L2TP	17803	L2TP connection established
	17804	L2TP connection terminated
PPTP	17805	PPTP connection established
	17806	PPTP connection terminated
IPsec	17801	IPsec connection established
	17802	IPsec connection terminated

17832	Failover group activation successful. A particular connection/no connection established
17833	Failover successful
17834	Failover failed. Connection will be established on next failback event
17835	Failback successful
17836	Failback failed, revert back to current running connection successful
17837	Failback failed, revert back to current running connection also failed. Connection will be established on next failback event
17839	<connectionname>, activation: Connection activated successfully
17840	<connectionname>, activation: Failed to activate this connection. Reason: <reason>
17841	<connectionname>, activation: Trying to deactivate/initiate/terminate an inactive connection. Probable DB sync problem
17842	<connectionname>, EST-P1-MM: Response to establishment request from <peeris> peer <peerrequesterip> successful
17843	<connectionname>, EST-P1-MM: Response to establishment request from <peerrequesterip> failed because <reason>
17844	<connectionname>, EST-P1-AM: Response to establishment request from <peerrequesterip>, state # <state>
17845	<connectionname>, EST-P1-AM: Response to establishment request from <peerrequesterip> failed because <reason>
17846	<connectionname>, EST-P1-MM: Connection being initiated on request
17847	<connectionname>, EST-P1-AM: Connection with state <state> being initiated on request
17848	<connectionname>, EST-P1-MM: peer ID is <peerID>
17849	<connectionname>, EST-P1-AM: peer ID is <peerID>
17850	<connectionname>, EST-P1: Phase-1 ID mismatch. Configured peer ID is <remoteid> and received peer ID is <peerid>. System is initiator. Verify ID configuration at both the ends is in sync.
17851	<connectionname>, EST-P1: Phase-1 ID mismatch. No suitable connection for peer ID <peerid>. System is responder. Verify ID configuration at both the ends is in sync.
17852	<connectionname2>, EST-P1: Switched the connection from <connectionname> to <connectionname2> because a <connection name2>'s configuration matches the request better.
17853	<connectionname>, EST-P1: Peer did not accept any proposal sent. Reconfigure the connection on either of the ends

17854	<connectionname>, EST-P1: System did not accept any proposal received. Need to reconfigure the connection on either of the ends.
17855	<connectionname>, EST-P1: An error (mostly related to network) has occurred while sending a packet to advance the IKE state machine from state <state>.
17856	<connectionname>, EST-P1: Max number of retransmissions <count> reached STATE_MAIN_I1. No response (or no acceptable response) to first IKE message
17857	<connectionname>, EST-P1: Max number of retransmissions <count> reached STATE_MAIN_I3. Possible authentication failure or NAT device in between: no acceptable response to first encrypted message
17858	<connectionname>, EST-P1: Malformed payload in packet. Probable authentication failure (mismatch of pre-shared secrets). Verify pre-shared secrets are same at both the ends.
17859	<connectionname>, EST-P1: unexpected message received in state <state>. Payload received from the peer do not lead the system to the next expected IKE state
17860	<connectionname>, EST-P1: Informational exchange message is invalid because it has a previously used Message ID <messageid>
17861	<connectionname>, EST-P1-MM: Phase-1 SA initiated by peer is established
17865	<connectionname>, EST-P2: Initiating Phase-2 (protected by Phase-1 SA with <state>) on request with policy <policybits>
17866	<connectionname>, EST-P2: Initiating Phase-2 SA re-keying using Phase-1 SA <state>
17867	<connectionname>, EST-P2: Responding to a Phase-2 establishment request with message id <MESSAGE ID>
17868	<connectionname>, EST-P2: Max number of retransmissions <count> reached STATE_QUICK_I1. No acceptable response to our first Quick Mode message: perhaps peer likes no proposal
17869	<connectionname>, EST-P2: System require Perfect Forward Secrecy(PFS) but peer proposed not to use PFS
17870	<connectionname>, EST-P2: local subnet – Remote subnet configuration of the connection being initiated conflicts with that of an already established connection <establishedconnectionname>. Terminate connection <establishedconnectionname> before initiating.
17871	<connectionname>, EST-P2: System received a Phase-2 connection request whose local subnet – Remote subnet configuration conflicts with that of an already established connection <establishedconnectionname>. System is terminating connection <establishedconnectionname> to honour the incoming request.

17872	<connectionname>, EST-P2: A Phase-2 SA initiated by system is established.
17873	<connectionname>, EST-P2: A Phase-2 SA initiated by peer is established
17874	<connectionname>, NAT-T: No NAT device detected between local server and remote server
17875	<connectionname>, NAT-T: local server is behind a NAT device
17876	<connectionname>, NAT-T: Remote server is behind a NAT device
17877	<connectionname>, NAT-T: Both local and remote server are behind NAT devices
17878	<connectionname>, SA-MGT: Peer requested to delete Phase-1 SA. Deleting ISAKMP state <state>
17879	<connectionname>, SA-MGT: Peer requested to delete Phase-2 SA. Deleting IPsec state <state>
17880	<connectionname>, SA-MGT: Peer requested to delete Phase-2 SA. Deleting existing SA and re-initiate a new one. Replacing IPsec State #<state>
17881	<connectionname>, SA-MGT: Deleting remote access connection instance with peer <remoteinterfaceip>, isakmp=#<isakmp>, IPsec=#<IPsec>
17882	<connectionname>, SA-MGT: Deleting connection
17883	<connectionname>, SA-MGT: On deletion of connection, corresponding SA <state> is being deleted
17884	<connectionname>, SA-MGT: Initiating re-keying of connection 's Phase-1 (main mode) SA <state>
17885	<connectionname>, SA-MGT: Initiating re-keying of connection 's Phase-1 (aggresive mode) state <oldstate> to state <newstate>
17886	<connectionname>, SA-MGT: Phase 1 SA is being re-keyed
17887	<connectionname>, SA-MGT: Phase 2 SA is being re-keyed
17888	<connectionname>, SA-MGT: Phase 1 SA has expired
17889	<connectionname>, SA-MGT: Phase 1 SA has expired. Connection is configured not to re-key
17890	<connectionname>, SA-MGT: Phase 2 SA has expired
17891	<connectionname>, SA-MGT: Phase 2 SA has expired. Connection is configured not to re-key
17892	<connectionname>, DPD: Dead peer detection enabled
17893	<connectionname>, DPD: Peer was unreachable and was marked as dead for this connection
17894	<connectionname>, DPD: Connection was <actiononpeerdead> because peer was dead

	17895	<connectionname>, DPD: Connection was scheduled to be rekeyed because peer was unreachable and connection was re-initiated
	17896	<connectionname>, XAUTH: Sending username/password request
	17897	<connectionname>, XAUTH: User <user> attempting to login
	17898	<connectionname>, XAUTH: User <user> authenticated successfully
	17899	<connectionname>, XAUTH: User <user> failed to authenticate because <reason>
	17900	<connectionname>, XAUTH: received MODECFG message when in state <STATE NAME>, and appliance is not XAUTH client
	17901	<connectionname>, XAUTH: Username/password requested but connection configured as XAUTH client cannot be rekeyed. Turn off re-key for the connection
	17902	<connectionname>, XAUTH: XAUTH: Answering XAUTH challenge with user <user>
	17903	<connectionname>, XAUTH: Successfully authenticated. Appliance is XAUTH Client
	17939	Failed to send IPsec tunnel up/down notification mail
	17938	IPsec tunnel up/down notification mail sent successfully
Landing Page	17906	Landing page accepted
	17907	Landing page declined
WLAN	17908	Rogue AP scan successfully completed
	17909	Rogue AP scan failed
	17911	System triggered Rogue AP scan was initiated
CCC	17910	Failed to send heartbeat from appliance to CCC (reserved for use with CCC, no log is generated)
	17912	heartbeat sent from appliance to CCC (reserved for use with CCC, no log is generated)
	17918	Failed to send Keep-alive from appliance to CCC (reserved for use with CCC, no log is generated)
	17919	Keep-alive sent from appliance to CCC (reserved for use with CCC, no log is generated)
Appliance Access	17913	System blocked administrator account for login because of too many wrong login attempts
	17914	System unblocked administrator account
	17915	System locked administrator's session
HTTPS	17916	Unknown protocol traffic was denied
	17917	Invalid certificate was blocked
Guest User	17925	Guest user is added in system

	17926	Access details SMS sent to the SMS gateway for delivery to guest user
	17927	One or more guest users expired and auto-purged successfully
	17928	One or more guest users expired and auto-purged failed
	17929	One or more guest users expired and auto-purge partially failed
	17930	Failed to send access details SMS
Virtual Host	17935	Mapped server <server_ipaddress> is up/mapped server <server_ipaddress> is DOWN
CTA	17940	CTA started with active collectors
PPPoE	17953	<interface name>: PADO packet timeout no response from server.
	17954	<interface name>: Terminating session, reattempting in <seconds> Sec.
	17955	<interface name>: Discovery process completed
	17956	<interface name>: LCP link established
	17957	<interface name>: ISP not supporting LCP
	17958	<interface name>: Authentication successful
	17959	<interface name>: Authentication Fail. Please check username and password
	17960	<interface name>: Set interface IP < local IP>
	17961	<interface name>: Set gateway IP < remote IP>
	17962	<interface name>: Set Primary DNS < DNS IP if enable>
	17963	<interface name>: Set aux DNS < DNS IP>
	17964	<interface name>: PPPoE link up
	17965	<interface name>: PPPoE link down
	17966	<interface name>: Disconnect PPPoE due to LCP timeout
	17967	<interface name>: Disconnect PPPoE due to idle timeout
	17969	<interface name>: Reconnected on scheduled event.
PPTP	17972	LCP: Negotiation opening for < Client IP >
	17973	LCP: Link established for < Client IP >
	17974	< PAP/CHAP/MS-CHAPv2 > : Starting authentication
	17975	< PAP/CHAP/MS-CHAPv2 > : Authentication successful for user < user name >
	17976	< PAP/CHAP/MS-CHAPv2 > : Authentication failed for user < user name >
	17977	IPCP : IP allocated : < IP allocated >, IPCP : Set DNS : < Primary/secondary DNS server >, IPCP : Set WINS : < Primary/secondary WINS server >
	17978	LCP : Disconnect due to LCP timeout
	17979	STATS : Connect time : < connection time >, STATS : Sent < no. of bytes > bytes, received < no. of bytes > bytes

	17980	IPCP : Taking IPCP down for < Client IP > : < Reason >, LCP : Negotiation closing for <Client IP > : < Reason >, LCP : Negotiation closed for < Client IP >
	17981	IPCP : Taking IPCP down for < Client IP > : < Reason >, LCP : Negotiation closing for <Client IP > : < Reason >, LCP : Negotiation closed for < Client IP >
L2TP	17982	LCP : Negotiation opening for < Client IP >
	17983	LCP : Link established for < Client IP >
	17984	< PAP/CHAP/MS-CHAP > : Starting authentication
	17985	< PAP/CHAP/MS-CHAP > : Authentication successful for user < user name >
	17986	< PAP/CHAP/MS-CHAP > : Authentication failed for user < user name >
	17987	IPCP : IP allocated : < IP allocated >, IPCP : Set DNS : < Primary/secondary DNS server >, IPCP : Set WINS : < Primary/secondary WINS server >
	17988	LCP : Disconnect due to LCP timeout
	17989	STATS : Connect time : < connection time >, STATS : Sent < no. of bytes > bytes, received < no. of bytes > bytes
	17990	IPCP : Taking IPCP down for < Client IP > : < Reason >, LCP : Negotiation closing for <Client IP > : < Reason >, LCP : Negotiation closed for < Client IP >
	17991	IPCP : Taking IPCP down for < Client IP > : < Reason >, LCP : Negotiation closing for <Client IP > : < Reason >, LCP : Negotiation closed for < Client IP >
System	18000	Event
WC	17998	New firmware detected for <type>: <version>
	17999	[ <AP-ID>] unknown AP model encountered: <type>, dropping.
	18001	[<AP-ID>] no firmware available for AP type '<type>', dropping.
	18002	[ <AP-ID> ] device not authorized yet, dropping.
	18003	[ <AP-ID> ] corrupt payload. Device may have wrong key. Delete device to re-register it.
	18004	[ <AP-ID> ] sent firmware <firmware> to device, releasing connection.
	18005	[ <AP-ID> ] failed to send <firmware> to device, dropping.
	18006	[MASTER] sending notification about offline AP <AP>
	18007	Successfully sent config to AP [ <AP-ID> ].
	18008	Failed to send config to AP [ <AP-ID> ].
RED	18014	RED is connected
	18015	RED in disconnected
	18016	RED interim event

	18032	Red devices: Disabled: 5 Enabled: 15 Connected: 12 Disconnected 3
ATP	18017	ATP definitions upgraded from <old version> to <new version>
	18018	ATP definitions upgrade failed
SSL VPN clients	18019	SSL VPN clients upgraded from <old version> to <new version>
	18020	SSL VPN clients upgrade failed
IPsec clients	18021	IPsec clients upgraded from <old version> to <new version>
	18022	IPsec clients upgrade failed
Authentication clients	18023	Authentication clients upgraded from <old version> to <new version>
	18024	Authentication clients upgrade failed
RED firmware	18025	RED firmware upgraded from <old version> to <new version>
	18026	RED firmware upgrade failed
AP firmware	18027	AP firmware upgraded from <old version> to <new version>
	18028	AP firmware upgrade failed
up2date	18029	Failed to checked for updates
	18030	Failed to download file <MODULE>
WAF	18033	WAF rules upgraded from <old version> to <new version>
	18034	WAF rules upgrade failed

## Web Filter Logs

---

Logs are displayed only if Web Protection Module is subscribed.

Message ID	Message
16001	Transaction was allowed based on web policy rule
16002	Transaction was denied/blocked based on web policy rules
16003	HTTP File upload allowed
16004	Token override
16005	Transaction resulted in a warning being displayed to the end-user, based on web policy rules
16006	Transaction was allowed after the user proceeded through a warning
16007	HTTP file upload warned allowed
16008	Sandbox file allowed
16009	Sandbox file denied

## Module-specific Fields

Data Fields	Type	Description
time, date, timezone	string	System-local date/time at which the event occurred.
log_type	string	Log type. <code>log_type="Content Filtering"</code>
log_subtype	string	Action taken for the logged HTTP/HTTPS transaction.
user_name	string	End-user associated with the item being scanned.
user_gp	string	Group to which the user belongs.
iap	integer	Numerical ID of the web policy applied to this transaction.
src_ip, src_port	integer	IP address and port to which the HTTP/HTTPS connection was made.
dst_ip, dst_port	integer	IP address and port to which the HTTP/HTTPS connection was made.
protocol	string	IP protocol used for the connection.
category	string	Category of the URL being requested.
category_type	string	Classification associated with the category.
url	integer	URL being requested.
contenttype	string	MIME-type of the downloaded content.
override_token		
httpresponsecode	integer	Numeric HTTP response code.
sent_bytes	integer	Bytes sent upstream to the web server by the firewall.
recv_bytes	integer	Bytes received from the upstream web server by the firewall.
domain	string	FQDN part of the URL, representing the hostname/domain of the web site.
exceptions	string	List of the checks excluded by web exceptions.  av. Do not scan for malware.  https. Do not decrypt HTTPS traffic.  sandstorm. Do not check downloaded content with Sandstorm.  policy. Do not apply policy checks (for example, Allow/Warn/Block by Category, URL Group, Dynamic Category).

Data Fields	Type	Description
activityname	string	Name of a web policy activity that matched and caused the policy result. (If the transaction matches multiple activities then only the first one that causes the policy decision will be recorded.)
reason	string	For transactions that require Sandstorm analysis, records the Sandstorm status.  <code>eligible</code> . The file was identified as eligible for Sandstorm analysis but was excluded from analysis. This may be because Sandstorm was disabled in the firewall rule, in a filetype exclusion, in a web exception, or because Sandstorm is not licensed.  <code>not eligible</code> . The file was not eligible for Sandstorm analysis because it is not a risky type, or not a type which can be analyzed by the Sandstorm cloud service.  <code>pending</code> . The item required analysis in the cloud; the end-user was not able to download the item immediately.  <code>cached clean</code> . The file has been previously analyzed and is known to be clean.  <code>cloud clean</code> . The item was found to be clean after analysis in the cloud.  For all items sent to the Sandstorm cloud for analysis, there will be two entries in the “Content Filter” log: one with <code>reason="pending"</code> when the file is initially requested by the user, and one with <code>reason="cloud clean"</code> when the file is known to be OK to download. If the file is found to be malicious, it will be logged in the anti-virus log with <code>reason="cloud malicious"</code> .
log_id	integer	Numerical ID indicating the type of the message.
fw_rule_id	integer	ID number of the firewall policy rule that applies to this transaction.
transaction_id	integer	Indicates the AV scan's transaction ID. This will only appear when malware/content scanning has been performed in that transaction.

## Application Filter Logs

---

Logs are displayed only if Web Protection Module is subscribed.

Message ID	Message
17051	Application access was denied according to application filter policy

### Module-specific Fields

Data Fields	Type	Description
fw_rule_id	integer	Firewall Rule ID which is applied on the traffic
user	string	User name
user_group	string	Group name to which the user belongs.
application_policy_id	integer	Application Filter Policy ID applied on the traffic
category	string	Name of the category under which application falls
app_name	string	Name of the application accessed
app_risk	integer	Risk level assigned to the application 1 - VERY LOW 2 - LOW 3 - MEDIUM 4 - HIGH 5 - VERY HIGH
app_technology	string	Technology of the application Browser Based Client Server Network Protocol P2P
application_category	string	Name of the category under which application falls
src_ip	string	Original Source IP address of traffic
src_country	string	Code of the country to which the source IP belongs
dst_ip	string	Original Destination IP address of traffic
dst_country	integer	Code of the country to which the destination IP belongs
protocol	integer	Protocol number of traffic
src_port	integer	Original Source Port of TCP and UDP traffic

Data Fields	Type	Description
dst_port	integer	Original Destination Port of TCP and UDP traffic
bytes_sent	integer	Total number of bytes sent
bytes_received	integer	Total number of bytes received
status	string	Ultimate state of traffic – accept/deny
message	string	Message displayed
appresolvedby	string	Application is resolved by signature or synchronized applications

## Malware Logs

---

**HTTP, HTTPS, FTP Logs are displayed only if Web Protection Module is subscribed.**

**POP, POPS, IMAP, IMAPS, SMTP and SMTPS Logs are displayed only if Web Protection Module is subscribed.**

Message ID	Message	Log Component
08001	The URL has been blocked as it contained a virus	HTTP
08002	Access to URL is allowed as it does not contain any virus	HTTP
09001	FTP data transfer was blocked as it contained a virus	FTP
09002	FTP data transfer didn't have any virus and completed successfully	FTP
10001	The mail is infected with a virus detected by the Device	SMTP
10002	Mail doesn't contain any virus	SMTP
11001	The mail is infected with a virus detected by the Device	POP3
11002	Mail doesn't contain any virus	POP3
12001	The mail is infected with a virus detected by the Device	IMAP4
12002	Mail doesn't contain any virus	IMAP4

## Module-specific Fields

Data Fields	Type	Description
time, date, timezone	string	System-local date/time at which the event occurred.
log_component	string	Application protocol or firewall component that detected the malware.
log_subtype	string	log_subtype="Virus"

Data Fields	Type	Description
status		
user_name	string	End-user associated with the item being scanned.
iap	integer	Numerical ID of the web policy applied to this transaction.
av_policy_name	string	
src_ip, src_port	integer	IP address and port from which the connection originated (client-side).
dst_ip, dst_port	integer	IP address and port to which the connection is directed (server-side).
virus	string	Name of the malware identified by the scan engine.
url	string	Protocol-specific information about the event.
domain_name	string	FQDN part of the URL.
dst_country_code	string	GeoIP country code associated with the destination IP address.
log_id	integer	Numerical ID indicating the type of the message.
sent_bytes	integer	Data, in bytes, sent by the firewall to the destination.
recv_bytes	integer	Data, in bytes, received.

## Email Logs

Logs are displayed only if Email Protection Module is subscribed.

Message ID	Message	Protocol
13001	A mail considered to be a SPAM	SMTP
13002	A mail considered to be a PROBABLE SPAM	
13003	A mail was not considered SPAM or PROBABLE SPAM	
13004	Sender IP address is blacklisted.	
13005	A mail considered to be an Outbound SPAM	
13006	A mail considered to be an Outbound Probable SPAM	
13007	Flagged clean by both IBS/OBS	
13008	Message is marked clean by outbound	
13009	DLP detected in mail	
13010	SPX successfully applied	
13011	SPX failed	
13012	SMTP DOS	

Message ID	Message	Protocol
13013	Email is marked Clean by Sophos Sandstorm	
13014	Email is marked Malicious by Sophos Sandstorm	
14001	A mail considered to be a SPAM	
14002	A mail considered to be a PROBABLE SPAM	POP
14003	A mail was not considered SPAM or PROBABLE SPAM	
15001	A mail considered to be a SPAM	
15002	A mail considered to be a PROBABLE SPAM	IMAP
15003	A mail was not considered SPAM or PROBABLE SPAM	

## Module-specific Fields

Data Fields	Type	Description
status	string	Ultimate status of traffic – Allowed or Denied
firewall_rule_id	integer	Firewall Rule ID which is applied on the traffic
user	string	User name
policy_name	string	Spam policy name which is applied on the traffic
sender	string	Sender email address
recipient	string	Recipient email address
subject	string	Email subject
message_id	string	Email ID
email_size	string	Email size
action	string	Action performed on the message  Possible values: Reject Drop Accept Change Recipient Prefix subject Sandstorm Allow Sandstorm Deny
reason	string	Reason why email was detected as spam/malicious
host	string	Sender domain name
domain	integer	Receiver domain name
src_ip	string	Original Source IP address of traffic
src_country	string	Code of the country to which the source IP belongs
dst_ip	string	Original Destination IP address of traffic
dst_country	string	Code of the country to which the destination IP belongs

Data Fields	Type	Description
protocol	integer	Protocol number of traffic
src_port	integer	Original Source Port of TCP and UDP traffic
dst_port	integer	Original Destination Port of TCP and UDP traffic
bytes_sent	integer	Total number of bytes sent
bytes_received	integer	Total number of bytes received
quarantine_reason	string	Reason for the quarantine mail

## Firewall Logs

---

Message ID	Message
00001	Firewall traffic allowed
00002	Firewall traffic denied
00003	Firewall traffic dropped by Galileo Heartbeat
00004	ICMP-related packets denied
00005	ICMP-related packets allowed
00007	Allowed missing heartbeat traffic in case of no restriction
01001	Invalid traffic dropped
01301	Fragmented traffic denied
01601	Invalid fragmented traffic denied
02001	Local ACL traffic allowed
02002	Local ACL traffic denied
03001	DoS attack dropped
04001	ICMP-redirected packet dropped
05001	Source-routed packet dropped
05051	Foreign host denied
05101	IPMAC pair denied
05151	IP Spoof denied
05201	SSL VPN resource access denied
05301	ARP Flood traffic denied
05401	Traffic for virtual host <virtualhostname> is denied. No Internal server is available to process the traffic.
010202100	Invalid packet.
010202101	IP packet with invalid header.
010202102	IP packet with invalid header version.
010202103	IP packet with invalid header time-to-live.
010202104	IP packet with invalid header protocol.
010202105	Truncated/malformed IP packet.

Message ID	Message
010202106	Bad IP checksum.
010202107	IP packet with invalid address(es).
010202108	Invalid IP fragment.
010202109	Short ICMP packet.
010202110	Bad ICMP checksum.
010202111	ICMP packets with invalid ICMP type/code.
010202112	Invalid packet, no ICMP record found.
010202113	ICMP packet error.
010202114	Short UDP packet.
010202115	Truncated/malformed UDP packet.
010202116	Bad UDP checksum.
010202117	Invalid UDP destination.
010202118	Short TCP packet.
010202119	Truncated/malformed TCP packet.
010202120	Bad TCP checksum.
010202121	TCP packets with invalid flag combination.
010202122	Invalid TCP state.
010202123	Invalid TCP RST.
010202124	Invalid TCP source port.
010202125	Invalid TCP destination port.
010202126	TCP land attack.
010202127	Invalid TCP reserved bit.
010202128	TCP winnuke attack.
010202129	Could not associate packet with any connection.
010202130	FTP-bounce attack.
010202131	Short UDPLite packet.
010202132	Bad UDPLite checksum.
010202133	UDPLite checksum is missing.
010202134	Invalid DCCP packet.
010202135	Invalid DCCP state.
010202136	Short DCCP packet.
010202137	Truncated/malformed DCCP packet.
010202138	Bad DCCP checksum.
010202139	Invalid DCCP reserved packet.
010202140	Invalid connection helper.
010202141	Packet discarded.

## Module-specific Fields

Data Fields	Type	Description
status	string	Ultimate status of traffic – Allowed or Denied
con_duration	integer	Duration of connection (in seconds)
fw_rule_id	integer	Firewall Rule ID which is applied on the traffic
user	string	User name
user_group	string	Group name to which the user belongs
web_policy_id	integer	Internet Access policy ID applied on the traffic
ips_policy_id	integer	IPS policy ID applied on the traffic
appfilter_policy_id	Integer	Application Filter policy applied on the traffic
app_name	string	Application name
app_risk	integer	Risk level assigned to the application
		<b>Possible values:</b>
		1 - VERY LOW
		2 - LOW
		3 - MEDIUM
		4 - HIGH
		5 - VERY HIGH
app_technology	string	Technology of the application
		<b>Possible values:</b>
		Browser Based
		Client Server
		Network Protocol
		P2P
app_category	string	Name of the category under which application falls
in_interface	string	Interface for incoming traffic, e.g., Port A
out_interface	string	Interface for outgoing traffic, e.g., Port B
src_ip	string	Original source IP address of traffic
src_mac	string	Original source MAC address of traffic
src_country	string	Code of the country to which the source IP belongs
dst_ip	string	Original destination IP address of traffic
dst_country	string	Code of the country to which the destination IP belongs
protocol	integer	Protocol number of traffic
src_port	integer	Original source port of TCP and UDP traffic
dst_port	integer	Original destination port of TCP and UDP traffic
icmp_type	integer	ICMP type of ICMP traffic
icmp_code	integer	ICMP code of ICMP traffic

Data Fields	Type	Description
packets_sent	integer	Total number of packets sent
packets_received	integer	Total number of packets received
bytes_sent	integer	Total number of bytes sent
bytes_received	integer	Total number of bytes received
src_trans_ip	integer	Translated source IP address for outgoing traffic. It is applicable only in route mode.
		<b>Possible values</b>
		"" - When appliance is deployed in Bridge mode or source IP translation is not done.
		IP Address - IP address with which the original source IP is translated.
src_trans_port	integer	Translated source port for outgoing traffic. It is applicable only in route mode.
		<b>Possible values</b>
		"" - When appliance is deployed in Bridge mode or source port translation is not done.
		Port - Port with which the original port is translated.
dst_trans_ip	integer	Translated destination IP address for outgoing traffic. It is applicable only in route mode.
		<b>Possible values</b>
		"" - When appliance is deployed in Bridge mode or destination IP translation is not done.
		IP Address - IP address with which the original destination IP is translated.
dst_trans_port	integer	Translated destination port for outgoing traffic. It is applicable only in route mode.
		<b>Possible values</b>
		"N/A" - When appliance is deployed in Bridge mode or destination port translation is not done.
		Port - Port with which the original port is translated.
src_zone_type	string	Type of source zone, e.g., LAN
src_zone	string	Name of source zone
dst_zone_type	string	Type of destination zone, e.g., WAN
dst_zone	string	Name of destination zone
con_direction	string	Packet direction. Possible values: "org", "reply", ""
con_event		Event on which this log is generated
con_id	integer	Unique identifier of connection
virt_con_id	integer	Connection ID of the master connection
hb_status	string	Status of heartbeat traffic

## IPS Logs

---

Logs are displayed only if Network Protection Module is subscribed.

Message ID	Message
06001	IPS Anomaly detected
06002	IPS Anomaly dropped
07001	IPS Signature detected
07002	IPS Signature dropped

### Module-specific Fields

Data Fields	Type	Description
status	string	Ultimate status of traffic – Allowed or Denied
idp_policy_id	integer	IPS policy ID which is applied on the traffic
idp_policy_name	integer	IPS policy name i.e. IPS policy name which is applied on the traffic
fw_rule_id	integer	Firewall Rule ID which is applied on the traffic
user	string	User name
sig_id	string	Signature ID
message	string	Signature message
classification	string	Signature classification
rule_priority	string	Priority of IPS policy
src_ip	string	Original Source IP address of traffic
src_country	string	Country Code of country from where traffic has originated.
dst_ip	string	Original Destination IP address of traffic
dst_country	string	Country Code of country to where traffic is destined.
protocol	integer	Protocol number of traffic
src_port	integer	Original Source Port of TCP and UDP traffic
dst_port	integer	Original Destination Port of TCP and UDP traffic
icmp_type	integer	ICMP type of ICMP traffic
icmp_code	integer	ICMP code of ICMP traffic

Data Fields	Type	Description
OS	string	<p>Platform of the traffic.</p> <p><b>Possible values:</b></p> <ul style="list-style-type: none"> <li>Windows</li> <li>Linux</li> <li>Unix</li> <li>MAC</li> <li>Solaris</li> <li>BSD</li> <li>Other</li> </ul>
category	string	<p>IPS signature category.</p> <p><b>Possible values:</b></p> <ul style="list-style-type: none"> <li>Apache HTTP Server</li> <li>Application and Software</li> <li>Browsers</li> <li>Database Management Systems</li> <li>DNS</li> <li>ERP Systems</li> <li>Exchange Mail Server</li> <li>FTP</li> <li>Industrial Control Systems</li> <li>Malware Communication</li> <li>Microsoft IIS Web Server</li> <li>Misc</li> <li>Multimedia</li> <li>Office Tools</li> <li>Operating System and Services</li> <li>Other Mail Server</li> <li>Other Web Server</li> <li>Reconnaissance</li> <li>Sendmail</li> <li>VoIP and Instant Messaging</li> <li>Web Services and Applications</li> </ul>
victim	string	<p>IPS traffic target.</p> <p><b>Possible values:</b></p> <ul style="list-style-type: none"> <li>Client</li> <li>Server</li> </ul>

## Authentication Logs

Log Component	Message ID	Message
Firewall Authentication	17701	User logged in successfully to firewall
	17702	User failed to login to firewall
	17703	User logged out from firewall
	17945	Received challenge from <Auth Mech> server via <Client Type>.
My Account Authentication	17704	User logged in successfully to My Account
	17705	User failed to login to My Account
	17706	User logged out from Account
	17947	Received challenge from <Auth Mech> server via <Client Type>.
VPN Authentication	17707	User logged in successfully to VPN
	17708	User failed to login to VPN
	17709	User logged out from VPN
	17710	User logged in successfully to SSL VPN
SSL VPN Authentication	17711	User failed to login to SSL VPN
	17712	User logged out from SSL VPN
	17946	Received challenge from <Auth Mech> server via <Client Type>.
	17713	User logged in using Dial-In
Dial-In Authentication	17714	User failed to login using Dial-In
	17715	User logged out of Dial-In
	17948	NTLM enabled but AD server not configured
	17946	Cannot establish NTLM authentication channel with <server name>
NTLM	17950	NTLM authentication channel established successfully with <server name>
	17951	Cannot establish NTLM authentication channel with <server name>
	17952	NTLM authentication disabled from appliance access
External Authentication	17968	connection to ADS/LDAPS <server ip/fqdn> failed because <reason>

## Module-specific Fields

Data Fields	Type	Description
status	string	Ultimate status of traffic – Allowed or Denied

Data Fields	Type	Description
user	string	User name
user_group	string	Group name to which the user belongs.
client_used	string	Authentication client used
auth_mechanism	string	Mechanism used for authentication
reason	string	Reason to provide authentication
src_ip	string	Original Source IP address of traffic
src_mac	string	Original Source MAC address of traffic
bytes_sent	integer	Total number of bytes sent
bytes_received	integer	Total number of bytes received
message	string	Message displayed
name	string	Name of the user
event_timestamp	integer	timestamp

## Admin Logs

Message ID	Message
17501	Add operation
17502	Update
17503	Delete
17504	Other management action
17505	System - Maintenance actions
17506	Wizard
17507	Admin login logout
17504	<interface name>: Disconnect PPPoE due to Admin event
17970	Ha enable event
17971	Ha disable event
17504	PPTP/L2TP Service Enabled/Disabled Successfully

## Module-specific Fields

Data Fields	Type	Description
status	string	Ultimate status of traffic – Allowed or Denied
user	string	User name
src_ip	string	Original Source IP address of traffic
message	string	Message displayed

## Sandstorm Logs

---

Message ID	Message
13013	Sandstorm allowed
13014	Sandstorm denied
18041	A Sandstorm-eligible file was received or a file was found to be clean.
18042	The item will not be made available to the end-user. An error occurred during the Sandstorm process or the file was malicious.
18043	A file entered the “Pending” state awaiting submission and analysis.
16005	Website/file/application access is warned allowed according to the Internet access policy
16006	Website/file/application access is warned blocked according to the Internet access policy
16007	HTTP file upload warned allowed
16008	Sandstorm file allowed
16009	Sandstorm file denied
18009	Alert by ATP
18010	Drop by ATP
18012	Heartbeat status
18013	Endpoint status

## Web Server Protection (WAF) Logs

---

Logs are displayed only if Web Server Protection Module is subscribed.

Message ID	Message
17071	A web request is allowed by WAF
17072	A web request is blocked by WAF

## Advanced Threat Protection (ATP) Logs

---

Message ID	Message
18009	Alert by ATP
18010	Drop by ATP

## Security Heartbeat Logs

---

Logs are displayed only if Network Protection Module is subscribed.

Message ID	Message
18012	Heartbeat status
18013	Endpoint status

## Appendix B - IPS - Custom Pattern Syntax

---

Keyword	Value	Usage	
srcaddr/dstaddr	<ipaddress>;	The source/destination IP address	
sreport/dstport	<Number>;	The source/destination port	
content	"<content string>"; A string quoted within double quotes.	Multiple contents can be specified in one rule. The value can contain mixed text and binary data. The binary data is generally enclosed within the pipe ( ) character.	
nocase	Can be used with content keyword only	NULL	Ignore case in the content value
rawbytes	Can be used with content keyword only	NULL	Ignore any decoding. Look at the raw packet data
depth	Can be used with content keyword only	<number>; e.g. depth:5;	Look for the contents within the specified number of bytes of the payload. If the value of the depth keyword is smaller than the length of the value of the content keyword, this signature will never be matched
offset	Can be used with content keyword only	<number>; e.g. content:"cgi-bin/phf";offset:4;depth:20;	Start looking for the contents after the specified number of bytes of the payload. This tag is an absolute value in the payload. Follow the offset tag with the depth tag to stop looking for a match after the value specified by the depth tag. If there is no depth specified, continue looking for a match until the end of the payload.
distance	Can be used with content keyword only	<number>; For example content :"ABC";content:"DEF"; distance:1;	Search for the contents the specified number of bytes relative to the end of the previously matched contents. The distance tag could be followed with the within tag. If there is no value specified for the within tag, continue looking for a match until the end of the payload.
within	Can be used with content keyword only	<number>; For example content:"ABC";content:"DEF";within:1	Look for the contents within the specified number of bytes of the payload. Use with the distance tag.

Keyword	Value	Usage
uricontent	uricontent:<content string>; For exampleuricontent:"%3F";	Search for the normalized request URI field. Binary data can be defined as the URI value.
isdataat	<value> [,relative]; For examplecontent:"PASS";isdataat:50,relative;	Verify that the payload has data at a specified location. Optionally look for data relative to the end of the previous content match.
pcre	pcre:[!]"(/<regex>/ m/<regex>/)[ismxAEGRUB]"; For examplepcre:"/BLAH/i";	<p>The pcre keyword allows rules to be written using perl compatible regular expressions.</p> <p><b>i</b> - Case insensitive</p> <p><b>s</b> - Include newlines in the dot metacharacter</p> <p><b>m</b> - By default, the string is treated as one big line of characters^ and \$ match at the start and end of the string. When m is set, ^ and \$ match immediately following or immediately before any newline in the buffer, as well as the very start and very end of the buffer.</p> <p><b>x</b> - Whitespace data characters in the pattern are ignored except when escaped or inside a character class</p> <p><b>A</b> - The pattern must match only at the start of the buffer (same as ^)</p> <p><b>E</b> - Set \$ to match only at the end of the subject string. Without E, \$ also matches immediately before the final character if it is a newline (but not before any other newlines)</p> <p><b>G</b> - Inverts the "greediness" of the quantifiers so that they are not greedy by default, but become greedy if followed by "?"</p> <p><b>R</b> - Match relative to the end of the last pattern match (similar to distance:0;) U Match the decoded URI buffers (similar to the uri keyword)</p> <p><b>B</b> - Do not use the decoded buffers (similar to the raw keyword)</p>

Keyword	Value	Usage
byte_test	<bytes to convert>, [!]<operator>, <value>, <offset> [,relative] [,<endian>] [,<number type>, string]; oct,dec,hex used with string only For example msg:"AMD procedure 7 plog overflow"; content:" 00 04 93 F3 "; content:" 00 00 00 07 "; distance:4.within:4;byte_test:4,>,1000,2  <b>operator</b> ,The operation to perform to test the value (<,>=,!,&)  <b>value</b> - The value to test the converted value against  <b>offset</b> - The number of bytes into the payload to start processing  <b>relative</b> - Use an offset relative to last pattern match  <b>big</b> - Process the data as big  <b>endian (default) little</b> - Process the data as little endian  <b>string</b> - The data is stored in string format in the packet  <b>hex</b> - The converted string data is represented in hexadecimal  <b>dec</b> - The converted string data is represented in decimal  <b>oct</b> - The converted string data is represented in octal	Test a byte field against a specific value (with operator). Capable of testing binary values or converting representative byte strings to their binary equivalent and testing them.  bytes_to_convert - The number of bytes to pick up from the packet  operator,The operation to perform to test the value (<,>=,!,&)  value - The value to test the converted value against  offset - The number of bytes into the payload to start processing  relative - Use an offset relative to last pattern match  big - Process the data as big  endian (default) little - Process the data as little endian  string - The data is stored in string format in the packet  hex - The converted string data is represented in hexadecimal  dec - The converted string data is represented in decimal  oct - The converted string data is represented in octal

Keyword	Value	Usage
byte_jump	<bytes_to_convert>, <offset> [,relative] [,multiplier <multiplier value>] [,big] [,little][,string] [,hex] [,dec] [,oct] [,align] [,from_beginning]; oct,dec,hex used with string only For examplecontent:" 00 00 00 01 ";distance:4;within:4;byte_jump:4,12,relative,align	<b>bytes_to_convert</b> - The number of bytes to pick up from the packet. <b>multiplier value</b> - multiply the number of calculated bytes by value and skip forward that number of byte <b>operator</b> - The operation to perform to test the value (<,>,=,!,&) <b>value</b> - The value to test the converted value against <b>offset</b> - The number of bytes into the payload to start processing <b>relative</b> - Use an offset relative to last pattern match <b>big</b> - Process the data as big <b>endian (default) little</b> - Process the data as little endian <b>string</b> - The data is stored in string format inthe packet <b>hex</b> - The converted string data is represented in hexadecimal <b>dec</b> - The converted string data is represented in decimal <b>oct</b> - The converted string data is represented in octal <b>align</b> – round the number of converted bytes upto the next 32 bit boundary <b>from_beginning</b> – Skip forward from the beginning of the packet payload instead of from the current position in the packet
ttl	<number>;<number>;<<number>;	Check the IP time-to-live value against the specified value
tos	<number>;	Check the IP TOS field for the specified Value
id	<number>;	Check the IP ID field for the specified Value

Keyword	Value	Usage
ipopts	{rr   eol   nop   ts   sec   lsrr  ssrr   satid   any}	<p><b>rr</b> - Check if IP RR (record route) option isPresent</p> <p><b>eol</b> - Check if IP EOL (end of list) option is present</p> <p><b>nop</b> - Check if IP NOP (no op) option is present</p> <p><b>ts</b> - Check if IP TS (time stamp) option is present</p> <p><b>sec</b> - Check if IP SEC (IP security) option is present</p> <p><b>lsrr</b> - Check if IP LSRR (loose source routing) option is present</p> <p><b>ssrr</b> - Check if IP SSRR (strict source routing) option is present</p> <p><b>satid</b> - Check if IP SATID (stream identifier) option is present</p> <p><b>any</b> - Check if IP any option is present</p>
fragoffset	<number>;	Allows to compare the IP fragment offset field against the decimal value
fragbits	[+*!]<[MDR]>;	<p>Check if IP fragmentation and reserved bits are set in the IP header.</p> <p><b>M</b> - The More Fragments bit</p> <p><b>D</b> - The Don't Fragment bit</p> <p><b>R</b> - The Reserved Bit</p> <p><b>+</b> - Match on the specified bits, plus any others</p> <p><b>*</b> - Match if any of the specified bits are set</p> <p><b>!</b> - Match if the specified bits are not set</p>
dsize	[<>] <number>[ <> number]; For example dsize:300<>400;	Test the packet payload size. With data_size specified, packet reassembly is turned off automatically so a signature with data_size and only_stream values set is wrong. dsize will fail on stream rebuilt packets, regardless of the size of the payload

Keyword	Value	Usage
flags	[! *] +]<FSRPAU120>[,<FSRPAU120>]; For exampleFlags:SF,12	Specify the TCP flags to match in a packet.  S - Match the SYN flag A - Match the ACK flag F - Match the FIN flag R - Match the RST flag U - Match the URG flag P - Match the PSH flag 1 - Match Reserved bit 1 2 - Match Reserved bit 2 0 - Match No TCP flags set + - Match on the specified bits, plus any others * - Match if any of the specified bits are set ! - Match if the specified bits are not set
flow	to_client to_server from_client  from_server ];established;bi_direction; [no_stream only_stream];	TCP only. The to_server value is from_server ].established;bi_direction; equal to the from_client value.  The to_client value is equal to the from_server value. The bi_direction tag makes the signature match traffic for both directions. For example, if you have a signature with "--dst_port 80", and with bi_direction set, the signature checks traffic from and to port 80.
seq	<number>;	Check for the specified TCP sequence number
ack	<number>;	Check for the specified TCP acknowledge number
window	<number>;	Check for the specified TCP window Size
itype	[<>]<number>[<>number];	Specify the ICMP type to match
icode	[<>]<number>[<>number];	Specify the ICMP code to match
icmp_id	<number>;	Check for the specified ICMP ID value
icmp_seq	<number>;	Check for the specified ICMP sequence Value

Keyword	Value	Usage
rpc	<application number>,[<version number> *],[<procedure number> *];	Check for RPC application, version, and procedure numbers in SUNRPCCALL requests. The * wildcard can be used for version and procedure numbers
ip_proto	<number>; [!]<number>;><number>;<<number>;	Check the IP protocol header
samip	NULL	The source and the destination have the same IP addresses

## Appendix C - Default File Type Categories

---

File Type Category Name	File Extensions	MIME Headers
Audio Files	gsm, sd2, qcp, kar, smf, midi, mid, ulw, snd, aifc, aif, aiff, m3url, m3u, wav, rm, au, ram, mp3, wmv	audio/x-gsm, audio/vnd.qcelp, audio/x-midi, application/x-midi, audio/midi, audio/x-mid, x-music/x-midi, audio/basic, audio/x-adpcm, audio/aiff, audio/x-aiff, audio/x-mpequrl, audio/wav, audio/x-wav, application/vnd.rn-realmedia, audio/x-au, audio/x-pn-realaudio, audio/mpeg3, audio/x-mpeg-3, audio/x-ms-wmv
Backup Files (The Backup Files category includes individual file backups and files related to backup software. Individual backup files are often generated automatically by software programs. Backup software files include incremental backups and full system backups.)	asd, bak, bkp, bup, dba, dbk, fbw, gho, nba, old, ori, sqb, tlg, tmp	application/octet-stream
Compressed Files(Compressed files use file compression in order to save disk space. Compressed archive formats can also be used to compress multiple files into a single archive.)	7z, alz, deb, gz, pkg, pup, rar, rpm, sea, sfx, sit, sitx, tar.gz, tgz, war, zip, zipx	application/x-7z-compressed, application/x-alz, application/x-deb, application/x-gzip, application/x-newton-compatible-pkg, application/x-rar-compressed, application/sea, application/x-sea, application/x-sit, application/x-stuffit, application/gnutar, application/x-compressed, application/x-zip-compressed, application/zip, multipart/x-zip

<b>File Type Category Name</b>	<b>File Extensions</b>	<b>MIME Headers</b>
Configuration Files(Settings files store settings for the operating system and applications. These files are not meant to be opened by the user, but are modified by the corresponding application when the program preferences are changed. Settings files may also be called preference files or configuration files.)	cfg, clg, dbb, ini, keychain, prf, prx, psf, rdf, reg, thmx, vmx, wfc	application/pics-rules, application/octet-stream, application/vnd.ms-officetheme
Database Files(Database files store data in a structured format, organized into tables and fields. Individual entries within a database are called records. Databases are commonly used for storing data referenced by dynamic websites.)	accdb, db, dsn, mdb, mdf, pdb, sql, sqlite	application/msaccess, application/x-msaccess, application/vnd.msaccess, application/vnd.ms-access, application/mdb, application/x-mdb, chemical/x-pdb
Developer Files (The Developer Files category contains files related to software development. These include programming project files, source code files, code libraries, header files, and class files. Compiled objects and components are also included in this category.)	as, asc, c, cbl, cc, class, cp, cpp, cs, csproj, dev, dtd, f, fs, fsproj, fsx, ftl, gem, h, hpp, ise, ism, java, m, ocx, pas, pod, pro, py, r, rb, sh, src, tcl, trx, v, vbproj, vcproj, vtm, xcodeproj	text/plain, text/x-c, application/java, application/java-byte-code, application/x-java-class, text/xml, text/x-fortran, text/x-h, text/x-javascript, text/x-m, application/octet-stream, text/pascal, text/x-script.phyton, application/x-bsh, application/x-sh, application/x-shar, text/x-script.sh, application/x-wais-source, application/x-tcl, text/x-script.tcl
Disk Image Files (Disk image files contain an exact copy of a hard disk or other type of media. They include all the files, as well as the file system information. This allows disk images to be used for duplicating disks, CDs, and DVDs. They are often used for backup purposes as well.)	dmg, iso, mdf, nrg, nri, pvm, toast, vcd, vmdk	application/x-cdlink

File Type Category Name	File Extensions	MIME Headers
Document Files(Document file format could be described as a text, or binary data file type, used to store formatted documents (texts, pictures, cliparts, tables, charts, multiple pages, multiple documents etc.).)	doc, docx, wbk, xls, xlsx, ppt, pptx, oft, pub, msg, one, xsf, xsn, grv, mpp, mpt, acl, pip, thmx, aw, bld, blg, bvp, cdd, cdf, contact, csv, dat, dif, dmusp, efx, epub, epw, exif, exp, fdb, fxp, gbr, gpi, hdf, id2, lib, mat, mcd, menc, mw, ndx, not, notebook, out, ovf, pdx, pfc, pps, ppsx, pptm, prj, qbw, sdf, svf, tar, tsv, vcf, vdb, vxml, windowslivecontact, wlmp, xfd, xml, xsl, xslt, lit, log, lst, odt, opml, pages, rtf, sig, tex, txt, wpd, wps, pdf	application/msword, application/vnd.openxmlformats-officedocument.wordprocessingml.document, application/excel, application/vnd.ms-excel, application/x-excel, application/x-msexcel, application/vnd.openxmlformats-officedocument.spreadsheetml.sheet, application/mspowerpoint, application/powerpoint, application/vnd.ms-powerpoint, application/x-mspowerpoint, application/vnd.openxmlformats-officedocument.presentationml.presentation, application/x-mspublisher, application/onenote, application/octet-stream, application/vnd.ms-project, application/x-project, application/vnd.ms-officetheme, application/cdf, application/x-cdf, application/x-netcdf, text/comma-separated-values, text/csv, application/csv, video/x-dv, application/x-hdf, application/mcad, application/x-mathcad, application/vnd.openxmlformats-officedocument.presentationml.slideshow, application/vnd.ms-powerpoint.presentation.macroEnabled.12, image/vnd.dwg, image/x-dwg, application/x-tar, text/tab-separated-values, text/x-vcard, application/xml, text/xml, application/x-ms-reader, text/plain, application/rtf, application/x-rtf, text/richtext, application/x-tex, application/wordperfect, application/x-wpwin, application/vnd.ms-works, application/pdf
Dynamic Files	pl, jsp, asp, php, cgi, shtml	text/x-script.perl, text/asp, text/x-server-parsed-html, text/html
Encoded Files (Encoded files are files that store data in an encoded format. These include encrypted files, uncompressed archives, and binary-encoded text files. Files are often encoded for security purposes and to keep them from being corrupted during data transfers.)	bin, enc, hex, hqx, mim, mime, uue	application/mac-binary, application/macbinary, application/octet-stream, application/x-binary, application/x-macbinary, application/binhex, application/binhex4, application/mac-binhex, application/mac-binhex40, application/x-binhex40, application/x-mac-binhex40, message/rfc822, www/mime, text/x-uuencode

File Type Category Name	File Extensions	MIME Headers
Executable Files	exe, cmd, bat, com	application/bat, application/x-bat, application/x-msdos-program, application/textedit, application/octet-stream, text/plain
Image Files	bmp, gif, jpeg, jpg, pcx, png	image/bmp, image/x-windows-bmp, image/gif, image/jpeg, image/png, image/x-pcx, image/png
Page Layout Files (Page layout files are documents that may contain both text and image data. They also include formatting information, which defines the page size, margins, and how content is organized on the page. Page layout documents are often used for creating printable publications, such as newspapers, magazines, and brochures.)	idml, indd, inx, isd, mdi, pct, pdf, pmd, ptx, pub, qxb, qxd, qxp, rels, xps	image/x-pict, application/pdf, application/x-mspublisher, application/octet-stream, application/vnd.ms-xpsdocument
Plugin Files (Plugin files provide extra features and functionality to existing programs. They are commonly used by image, video, and audio editing applications, as well as Web browsers. Plugins are also referred to as add-ons and extensions.)	8bi, arx, crx, plugin, vst, xll	application/x-visio, application/excel, application/vnd.ms-excel, application/x-excel
System Files (The System Files category includes files related to Mac, Windows, and Linux operating systems. Some examples include system libraries, icons, themes, and device drivers. Files output by the system are also included in this category.)	bashrc, cab, cpl, cur, dll, dmp, drv, hlp, ico, key, lnk, msp, prf, profile, scf, scr, sys	application/vnd.ms-cab-compressed, application/octet-stream, application/x-msdownload, application/hlp, application/x-helpfile, application/x-winhelp, image/x-icon
Video Files	dat, mov, avi, qt, smi, sml, smil, flc, fli, vfw, mpeg, mpg, m15, m1u, m1a, m75, mls, mp2, mpm, mp, rm, wmv, flv, swf	application/octet-stream, application/x-troff-msvideo, video/avi, video/msvideo, video/x-msvideo, video/quicktime, application/smil, application/x-simile, Video/flc, video/fli, video/x-fli, video/mpeg, video/x-mpeg, video/x-mpeq2a, application/vnd.rn-realmedia, video/flv, application/x-shockwave-flash
Web Files (The Web Files category includes files related to websites and Web servers. These include static and dynamic webpages, Web applications, and files referenced by webpages.)	alx, asax, asmx, aspx, atom, att, axd, chm, dwt	application/atom+xml

## Appendix E - Compatibility with SFMOS 15.01.0

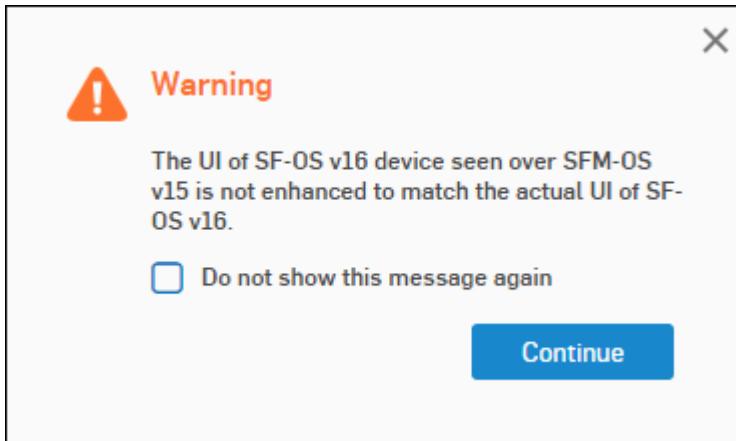
---

Please note that the following is applicable for Sophos Firewall device(s) above SFOS 16.01.0 if managed through SFMOS 15.01.0:

- With SFM-OS V15, you can only manage features of SF-OS V15 from group level. To manage SF-OS V16 features use device level view of SFM-OS V15.
- The UI of SF-OS V16 device seen over SFM-OS V15 is not enhanced to match the actual UI of SF-OS V16.



**Note:** You will see the following warning while opening device level view of any SF-OS V16 device from SFM-OS V15.



Click **Do not show this message again** on SFM if you do not want to see this warning again.

## Appendix F - Additional Documents

---

- [Command Reference Guide](#)
- [Reports Guide](#)
- [Software Appliance - Getting Started Guide](#)
- [Virtual Appliance - Getting Started Guide](#)
- [API Help](#)
- [Web Interface Reference and Admin Guide](#)
- [List of RED Supported 3G/4G/LTE USB Dongles](#)
- [Release Notes and guides to help with Cyberoam to XG Firewall migration](#)
- [How-to videos and guides to get started with XG Firewall](#)

## Copyright Notice

---

Copyright 2016-2017 Sophos Limited. All rights reserved.

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

No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise unless you are either a valid licensee where the

documentation can be reproduced in accordance with the license terms or you otherwise have the prior permission in writing of the copyright owner.