



# Cyberoam Central Console User Guide

Version 1

Document version 1.0-1.0-17/05/2007

## Important Notice

Elitecore has supplied this Information believing it to be accurate and reliable at the time of printing, but is presented without warranty of any kind, expressed or implied. Users must take full responsibility for their application of any products. Elitecore assumes no responsibility for any errors that may appear in this document. Elitecore reserves the right, without notice to make changes in product design or specifications. Information is subject to change without notice.

## USER'S LICENSE

The Appliance described in this document is furnished under the terms of Elitecore's End User license agreement. Please read these terms and conditions carefully before using the Appliance. By using this Appliance, you agree to be bound by the terms and conditions of this license. If you do not agree with the terms of this license, promptly return the unused Appliance and manual (with proof of payment) to the place of purchase for a full refund.

## LIMITED WARRANTY

**Software:** Elitecore warrants for a period of ninety (90) days from the date of shipment from Elitecore: (1) the media on which the Software is furnished will be free of defects in materials and workmanship under normal use; and (2) the Software substantially conforms to its published specifications except for the foregoing, the software is provided AS IS. This limited warranty extends only to the customer as the original licensee. Customers exclusive remedy and the entire liability of Elitecore and its suppliers under this warranty will be, at Elitecore or its service center's option, repair, replacement, or refund of the software if reported (or, upon, request, returned) to the party supplying the software to the customer. In no event does Elitecore warrant that the Software is error free, or that the customer will be able to operate the software without problems or interruptions. Elitecore hereby declares that the anti virus and anti spam modules are powered by Kaspersky Labs and the performance thereof is under warranty provided by Kaspersky Labs. It is specified that Kaspersky Lab does not warrant that the Software identifies all known viruses, nor that the Software will not occasionally erroneously report a virus in a title not infected by that virus.

**Hardware:** Elitecore warrants that the Hardware portion of the Elitecore Products excluding power supplies, fans and electrical components will be free from material defects in workmanship and materials for a period of One (1) year. Elitecore's sole obligation shall be to repair or replace the defective Hardware at no charge to the original owner. The replacement Hardware need not be new or of an identical make, model or part; Elitecore may, in its discretion, replace the defective Hardware (or any part thereof) with any reconditioned product that Elitecore reasonably determines is substantially equivalent (or superior) in all material respects to the defective Hardware.

## DISCLAIMER OF WARRANTY

Except as specified in this warranty, all expressed or implied conditions, representations, and warranties including, without limitation, any implied warranty or merchantability, fitness for a particular purpose, non-infringement or arising from a course of dealing, usage, or trade practice, and hereby excluded to the extent allowed by applicable law.

In no event will Elitecore or its supplier be liable for any lost revenue, profit, or data, or for special, indirect, consequential, incidental, or punitive damages however caused and regardless of the theory of liability arising out of the use of or inability to use the product even if Elitecore or its suppliers have been advised of the possibility of such damages. In the event shall Elitecore's or its supplier's liability to the customer, whether in contract, tort (including negligence) or otherwise, exceed the price paid by the customer. The foregoing limitations shall apply even if the above stated warranty fails of its essential purpose.

In no event shall Elitecore or its supplier be liable for any indirect, special, consequential, or incidental damages, including, without limitation, lost profits or loss or damage to data arising out of the use or inability to use this manual, even if Elitecore or its suppliers have been advised of the possibility of such damages.

## RESTRICTED RIGHTS

Copyright 2000 Elitecore Technologies Ltd. All rights reserved. Cyberoam, Cyberoam logo are trademark of Elitecore Technologies Ltd. Information supplies by Elitecore Technologies Ltd. Is believed to be accurate and reliable at the time of printing, but Elitecore Technologies assumes no responsibility for any errors that may appear in this documents. Elitecore Technologies reserves the right, without notice, to make changes in product design or specifications. Information is subject to change without notice

## Corporate Headquarters

Elitecore Technologies Ltd.

904 Silicon Tower,

Off. C.G. Road,

Ahmedabad – 380015, INDIA

Phone: +91-79-66065606

Fax: +91-79-26407640

Web site: [www.elitecore.com](http://www.elitecore.com), [www.cyberoam.com](http://www.cyberoam.com)

## Contents

<b>Introduction .....</b>	<b>5</b>
<b>Basics .....</b>	<b>6</b>
<b>Dashboard .....</b>	<b>8</b>
<b>System .....</b>	<b>10</b>
<b>Reset Console Password .....</b>	<b>10</b>
<b>Configure DNS .....</b>	<b>10</b>
<b>Manage Data .....</b>	<b>12</b>
Backup Data .....	12
Restore Data .....	12
<b>Device Group .....</b>	<b>13</b>
Create Group .....	13
Manage Group .....	14
<b>Device Management .....</b>	<b>16</b>
<b>Add Device .....</b>	<b>16</b>
<b>Manage Device .....</b>	<b>17</b>
<b>User .....</b>	<b>18</b>
<b>Create User .....</b>	<b>18</b>
<b>Manage User .....</b>	<b>19</b>
<b>Create Role .....</b>	<b>20</b>
<b>Manage Role .....</b>	<b>21</b>
<b>Firewall .....</b>	<b>22</b>
<b>Create Firewall Rule .....</b>	<b>24</b>
<b>Manage Firewall Rules .....</b>	<b>31</b>
<b>Host .....</b>	<b>33</b>
Add Host .....	33
Manage Host .....	33
<b>Host Group .....</b>	<b>35</b>
Create Host Group .....	35
Manage Host Group .....	35
<b>Services .....</b>	<b>38</b>
Create Service .....	38
Manage Service .....	39
<b>Categories .....</b>	<b>42</b>
<b>Web Category .....</b>	<b>43</b>
Create Custom Web category .....	43
Manage Custom Web category .....	46
Manage Default Web category .....	48
<b>File Types Category .....</b>	<b>54</b>
Create Custom File Type category .....	54
Manage Custom File Type category .....	55
Manage Default File Type category .....	55
<b>Application Protocol Category .....</b>	<b>56</b>

Create Custom Application Protocol category .....	56
Manage Custom Application Protocol category .....	58
Manage Default Application protocol category .....	59
<b>Policies .....</b>	<b>60</b>
<b>Schedule .....</b>	<b>60</b>
Define Schedule .....	60
Manage Schedule .....	62
<b>Internet Access Policy .....</b>	<b>65</b>
Create Policy .....	65
Manage Policy .....	69
<b>Bandwidth Policy .....</b>	<b>71</b>
Create Policy .....	72
Manage Policy .....	76
<b>IDP .....</b>	<b>78</b>
<b>Policy .....</b>	<b>78</b>
Create IDP Policy .....	79
Manage IDP Policy .....	83
<b>Custom Signatures .....</b>	<b>85</b>
Create Custom Signature .....	85
Manage Custom Signature .....	87
<b>Help .....</b>	<b>89</b>
<b>Upload Upgrade .....</b>	<b>89</b>
<b>Licensing .....</b>	<b>89</b>

# Introduction

Cyberoam Central Console is an integrated management and monitoring tool allows to manage multiple, dispersed Cyberoam Installations centrally. It establishes a central point for monitoring and maintaining multiple Cyberoam Installations.

Cyberoam Central Console helps Managed Security Service Providers, Enterprises – multiple branch offices same city multiple locations or in different Cities and Universities – multiple departments same campus or multiple campuses to manage and monitor their multiple Cyberoam Installations centrally.

Cyberoam Central Console is an independent and a separate hardware from Cyberoam i.e. not the part of Cyberoam Appliance, is to be purchased, installed, and registered separately.

Cyberoam Central Console is to be registered before use.

Cyberoam Central Console supports role-based administration. Permissions for Cyberoam Appliances (devices) and Cyberoam Central Console configuration and management can be set individually for each administrative user added to Cyberoam Central Console.

Administrators with local permission can configure and manage Cyberoam Central Console as well as following functions of Cyberoam appliances:

- Firewall rule
- Internet Access policy
- Bandwidth policy
- IDP policy
- Categories

Administrators without local permission can manage Cyberoam appliances only and not Cyberoam Central Console.

Prerequisite: Each Cyberoam Appliance should allow HTTPS access for Cyberoam Central Console

## Basics

Cyberoam Central Console can be accessed and administered from:

1. Web Admin Console
2. Telnet Console

### Web Admin Console

Web Admin Console provides access to all the configuration and maintenance functions of Cyberoam Central Console.

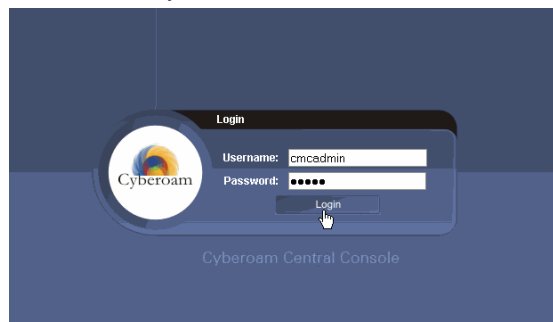
It is mainly used for:

3. Adding Appliances which are to be managed by Cyberoam Central Console
4. Configuring and managing Cyberoam Internet Access, Bandwidth and IDP policies
5. Configuring and managing Cyberoam Firewall rules
6. Configuring and managing Cyberoam Categories
7. Creating and managing Cyberoam Custom IDP signature

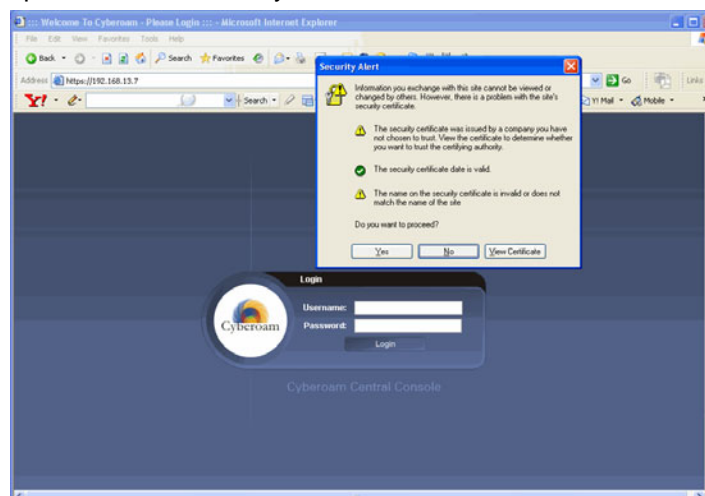
Only configuration required on Cyberoam Central Console is the registration of all the Cyberoam Appliances that are to be managed and monitored through Cyberoam Central Console. To register a Cyberoam Appliance with Cyberoam Central Console, one needs to add IP address, administrator Username and password of Cyberoam.

Web Admin Console can be accessed using HTTP or a secure HTTPS connection from any computer using web browser as:

1. HTTP login: `http://<IP address of Cyberoam Central Console >`



2. HTTPS login: `https://<IP address of Cyberoam Central Console>`





**Microsoft Internet Explorer 5.5 or Mozilla Firefox 1.5+ and Display settings as True color (32 bits) is required to access Web Admin Console**

**Use the default username “admin” and password “admin” if you are logging to Web Admin Console for the first time after installation**

When you log on to Web Admin Console, Dashboard is displayed.

Dashboard helps to watch all the registered Cyberoam Appliances for outages and events that requires attention. Cyberoam Central Console gets all the required information from Cyberoam Appliances which is displayed on Dashboard. This saves you from time consuming manual monitoring of multiple Cyberoam Appliances individually.

The button bar on the upper rightmost corner provides access to online help and license information about Cyberoam Central Console. Use Logout button to log out from the Web Admin Console.

#### **View License information**

Click CCC icon (on the rightmost corner of the screen) to view the license information.

It displays installed version of Cyberoam Central Console, appliance key and Model number. If Cyberoam Central Console is registered, it displays name under which Cyberoam Central Console is registered.



**Use F2 key to return to home page**

#### **Telnet Console**

It is mainly used for

1. Configuring Network and System
2. Managing Cyberoam Application

Telnet Console can be accessed via remote login utility – TELNET as:

TELNET login: TELNET IP Address of the Cyberoam Central Console

Refer to Console Guide on how to configure Cyberoam from Telnet Console.



**Default password for Telnet Console is “admin”**

#### **Accessing Console using SSH client**

Access Cyberoam Console using any of the SSH client. Cyberoam Central Console server IP Address is required.

Start SSH client and create new Connection with the following parameters:

Hostname - <Cyberoam Central Console server IP Address>

Username – admin

Password – admin

## Dashboard

As soon as you logon to the Web Admin Console, Group level Dashboard is displayed.

The goal of dashboard is to provide fast access to monitor and analyze all the registered Cyberoam Appliances for outages and events that requires attention. Cyberoam Central Console gets all the required information from Cyberoam Appliances which is displayed on Dashboard. This saves you from time consuming manual monitoring of multiple Cyberoam Appliances individually.

Dashboard displays live status / severity of following parameters of all the registered Cyberoam Appliances:

- Connectivity – Connectivity of Cyberoam with Cyberoam Central Console and connectivity of Cyberoam with its gateway (Mostly in case of Multiple gateway in Cyberoam)
- IAP trends
- IDP Threats – Severity depends on number of events generated in last 5 minutes
- Virus Attack – Severity depends on % of Viruses detected with respect to total number of sites visited and mails received
- Spam Mails – Severity depends on % of SPAM mails received with respect to the total mails received
- Version Compatibility – Cyberoam Central Console will not be able to manage Cyberoam if not compatible, either Cyberoam Central Console/Cyberoam needs to be upgraded
- Subscription - Severity depends on number of days left in expiration for any module

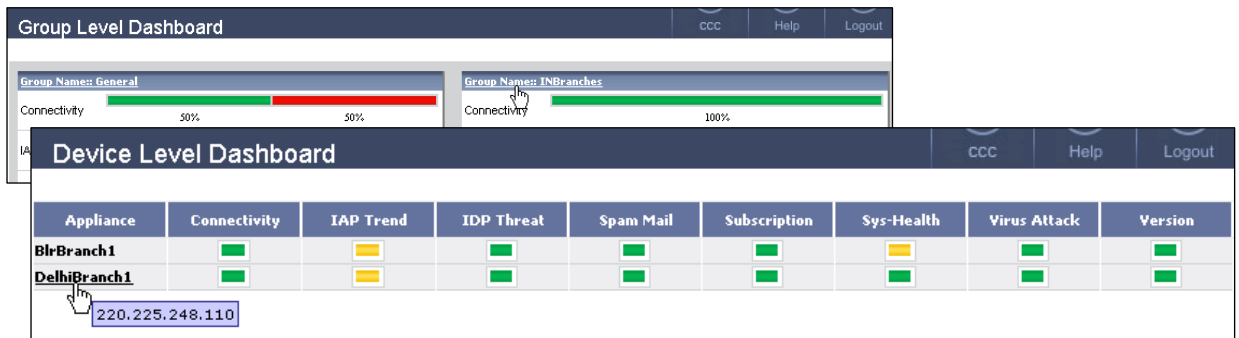
Status and severity are classified as Dangerous, Warning, OK which is based on the preconfigured threshold values in Cyberoam Central Console.

- Group Level Dashboard displays the Group activity and not the individual Cyberoam activity, if Device Groups are created.





- Device Level Dashboard displays status of individual Cyberoam Appliance in a respective group. Click Group Name on Group Level Dashboard to view Device Level Dashboard.



- Click Appliance link from Device Level Dashboard to view the Device Summary. Device summary includes
  - Cyberoam Appliance information – Appliance key, model, Deployment mode, version, etc.
  - Connection date and time i.e. date and time when connection between Cyberoam and Cyberoam Central Console was established.
  - Internet access trends
  - IDP threats – threats within last 5 minutes
  - Spam mails – spam mails received as a percentage of the total mails received
  - Virus attack details
  - System Health – CPU usage, memory and disk used as a percentage of the total amount of disk space available
  - Subscription/license information

Device Summary

ccc

Help

Logout

Detailed Information of 10.10.10.253

Appliance Name	CR253
IP Address	10.10.10.253
Appliance Key	C010600301-VF8V4D
Appliance Model	CR250i
Deployment Mode	Route
CMC Version	1.0.0.0
Cyberoam Version	9.4.2.0
Connected Since	May 02,2007 14:51:12
Connectivity	<div> <div>gw113</div> <div></div> </div>
IAP Trend	
Unhealthy	0%
Non-working	0%
Productive	0%
Neutral	0%
IDP Analysis	IDP Threats in Last 5 minutes are 0
SPAM Mails	60%
Virus Attack	
HTTP Virus	0%
Mail Virus	0%
System Health	
CPU	0%
Memory	64%
Disk Usages	1%
Subscription	
Web and Application Filter	23 Days Left
Intrusion Detection & Prevention	23 Days Left
Gateway Anti Virus	23 Days Left
Gateway Anti-spam	23 Days Left
8 x 5 Support	23 Days Left
24 x 7 Support	Unsubscribed

Connect

Cancel

# System

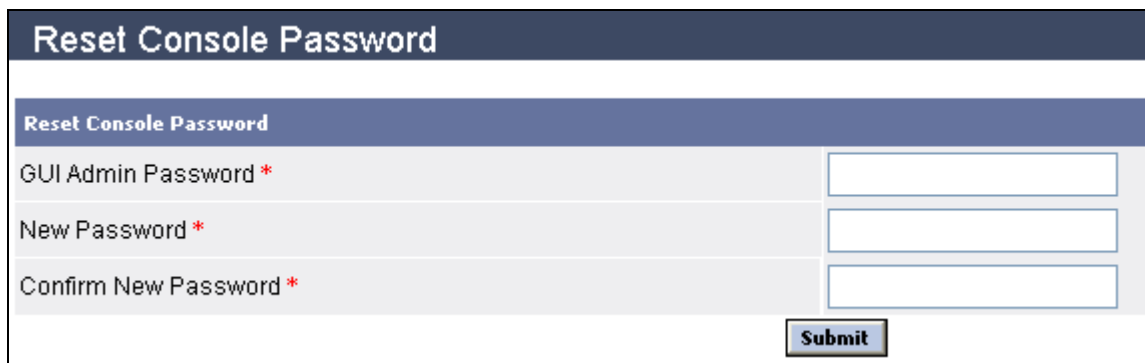
This section covers how to:

- Reset Console Password
- Configure DNS
- Manage Data

## Reset Console Password

Telnet Console password can be changed from Web Admin or Telnet Console.

1. Select **System** → **Reset Console Password**
2. Enter Web based Console's administrator user password using which you have logged on.
3. Enter new password
4. Enter the new password for confirmation. Use the same spelling and case as you entered in password field.
5. Click Submit to save the new password.



The screenshot shows a web form titled "Reset Console Password". The form has a header bar with the title. Below the header, there is a section titled "Reset Console Password" in a blue bar. The form contains three input fields: "GUI Admin Password \*" (with a red asterisk), "New Password \*" (with a red asterisk), and "Confirm New Password \*" (with a red asterisk). Each field has a corresponding text input box. At the bottom right of the form, there is a "Submit" button.

To change password from Telnet Console:

1. Log on to Telnet Console
2. Go to Option 2 - System Management > Option 1 - Set Console Password and change the password. For more details refer to Console guide.

## Configure DNS

DNS service allows provide internal users with a secure and efficient name-server service. A Domain Name Server translates domain names to IP addresses.

DNS server is set at the time of installation. You can add additional IP addresses of the DNS servers to which Cyberoam Central Console can connect for name resolution. You can even redirect DNS traffic to local DNS server.

If multiple DNS are defined, they are queried in the order as they are entered.

**To add DNS Server IP address**

1. Select **System → Configure DNS**
2. Click Add.
3. Enter DNS server IP address
4. Click OK
5. Click Save to save the configuration



**Do not forget to save after adding new IP address to the DNS list**

To add multiple DNS repeat the above-described procedure. Use Move Up & Move Down buttons to change the order of DNS. If more than one Domain name server exists, query will be resolved according to the order specified.

**To change the DNS order**

1. Select **System → Configure DNS**
2. Click the Server IP address whose order is to be changed
3. Click Move up or Move Down as per the requirement
4. Click Save to save the changes



**Do not forget to save after changing the order**

**To remove DNS Server**

1. Select **System → Configure DNS**
2. Click the Server IP address you want to remove
3. Click Remove
4. Click Save to save the changes



**Do not forget to save after removing IP address from the DNS list**



**Multiple DNS server can also be deleted. Select multiple servers using Ctrl key**

## Manage Data

- [Backup](#)
- [Restore Backup](#)

### Backup Data

1. Select **System → Manage Data → Backup Data**
2. Click Backup to take backup of System Data till date. A new window is opened automatically if backup is taken successfully to allow you to download the backup.  
Click Download and follow the screen instructions to download the backup file.
3. Displays the date and time of the last backup if backup is already taken.  
Click Download if you want to download backup for uploading.

Restore backup taken from System>Manage Data>Restore Data and upload the backup file.

### Restore Data

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

1. Select **System → Manage Data → Restore Data**
2. Enter the backup file name, which is to be uploaded.
3. Click Upload
4. Once the backup file is uploaded successfully, to restore data
5. Log on to Console based Administration (using TELNET).
6. Go to Option 5 – CCC Management > Option 4 – Restore Backup and follow screen steps to restore data. For more details, refer to Console Guide.

# Device Group

Cyberoam Central Console provides a quick way to configure a single device or a group of devices.

You can group the managed devices (Cyberoam Appliances) according to:

- Physical/geographic location e.g. devices in the same city
- Configurations e.g. devices which implements same policies
- Ownership e.g. devices under the single distributor, devices under a particular department in a university

Cyberoam Central Console allows configuring and managing following functions of Cyberoam appliances:

- Firewall rule
- Internet Access policy
- Bandwidth policy
- IDP policy
- Categories

- [Create Group](#)
- [Manage Group](#)

## Create Group

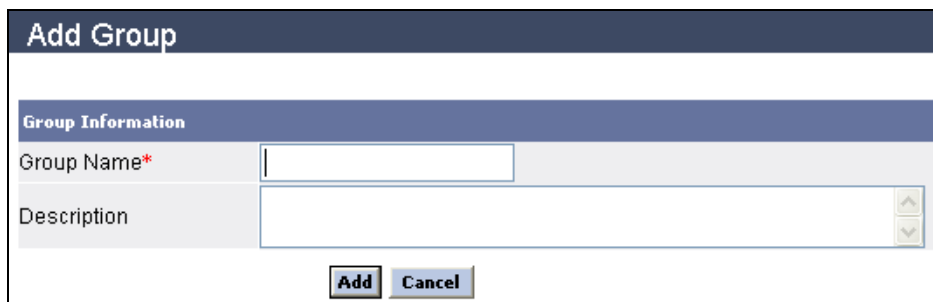
Creating Groups allows you to manage large number of devices efficiently. General group is the default group which cannot be deleted or updated

Use to:

- Create Group
- Update Group

## To create Group

1. Select **Device Group** → **Add Group**
2. Enter group name
3. Enter group description
4. Click Add to create and save the group



Add Group	
<b>Group Information</b>	
Group Name*	<input type="text"/>
Description	<div><div></div><div></div></div>
<div>Add Cancel</div>	

## To update Group

1. Select **Device Group → Manage Group** to view the list of groups created and click the group to be updated
2. Displays group name, modify of required
3. Displays group description, modify of required
4. Click Update to save the group

**Manage Group**

Group Name	Description
<b>General</b>	This is the D
<b>Ecore_CR</b>	
<b>Marketing_GRP</b>	

**Edit Group**

**Group Information**

Group Name\*

Description

## Manage Group

Use to:

- [Update Group](#)
- View list of devices in a Group
- Delete Group

## To view list of devices in a Group

1. Select **Device Group → Manage Group** to view the list of groups created
2. Click **+** against the group to expand the tree
3. Displays device name, IP address and connectivity status of all the device in a group

**Manage Group**

Group Name	Description
<b>General</b>	This is the Defa
<b>Ecore_CR</b>	
<b>Marketing_GRP</b>	

**Manage Group** Register CCC Help Logout

Group Name	Description	Del
<b>General</b>	This is the Default Group	<input type="checkbox"/>
<b>Ecore_CR</b>		<input type="checkbox"/>
Tech_CR	192.168.13.44	<input checked="" type="checkbox"/>
B_block	192.168.1.25	<input checked="" type="checkbox"/>
<b>Marketing_GRP</b>		<input type="checkbox"/>

Select All ☐

## To delete Group

1. Select **Device Group → Manage Group** to view the list of groups created
2. Click Del against the group to be deleted OR click Select All to delete all the groups
3. Click Delete

Manage Group

Register

CCC

Help

Logout

	Group Name	Description	Del
+	<u>General</u>	This is the Default Group	<input type="checkbox"/>
+	<u>Ecore_CR</u>		<input type="checkbox"/>
+	<u>Marketing_GRP</u>		<input checked="" type="checkbox"/>
			Select All <input type="checkbox"/>
			<div>Delete</div>

General Group is the default group which cannot be deleted.

# Device Management

Device Management allows to add devices i.e. Cyberoam Appliances that are to be managed through Cyberoam Central Console

Use to:

- Add Device i.e. register Device with Cyberoam Central Console
- Manage Device

## Add Device

Use to

- [Add Device](#) i.e. register Device with Cyberoam Central Console
- [Update Device details](#)

### To add Device

1. Select **Device Management → Add Device**
2. Enter device name and IP address
3. Enter username and password using which user can login to the Cyberoam Appliance
4. Enter device description, if required
5. Enter name, phone number and email id of Cyberoam Central Console administrator
6. Select device Group. If group is not selected then device is included in General group. You can change the group later on whenever required.
7. Click Add to register the device (Cyberoam Appliance) with Cyberoam Central Console

### Add Device

Device Information	
Device Name*	<input type="text"/>
Device IP*	<input type="text"/>
User Name*	<input type="text"/>
Password*	<input type="password"/>
Confirm Password*	<input type="password"/>
Description	<input type="text"/>
Local Admin Name	<input type="text"/>
Local Admin Phone No	<input type="text"/>
Local Admin Email ID	<input type="text"/>
Select Group	General <input type="button" value="v"/>



## To update Device details

1. Select **Device Management** → **Manage Device** to view the list of devices that are managed by Cyberoam Central Console and click the Device which is to be updated
2. Displays device name and IP address, modify if required
3. Displays username and password using which user can logon to the Cyberoam Appliance, modify if required
4. Displays device description, modify if required
5. Displays name, phone number and email id of Cyberoam Central Console administrator, modify if required
6. Displays device group, modify if required.
7. Click Update to save the details

**Manage Devices** ccc Help Logout

Device Name	IP Address	Appliancekey	Appliance Model	Deployment Mode	Version	Connectivity	Del
BlrBranch1	60.95.197.129	6095197129-1234567890	CR50i	Route	9.4.2.0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
DelhiBranch1	220.220.220.220	220220220220-1234567890	CR50i	Route	9.4.2.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>
USHeadOffice	100.100.100.100	100100100100-1234567890	CR100i	Route	9.4.2.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>

**Edit Device**

**Device Information**

Device Name\*

Device IP\*

User Name\*

Password\*

Confirm Password\*

Description

Local Admin Name

Local Admin Phone No

Local Admin Email ID

Select Group

## Manage Device

Use to

- [Update Device](#)
- Remove Device from Cyberoam Central Console

## To remove Device

1. Select **Device Management** → **Manage Device** to view the list of devices
2. Click Del against the device to be removed OR click Select All to remove all the devices
3. Click Delete

**Manage Devices** ccc Help Logout

Device Name	IP Address	Appliancekey	Appliance Model	Deployment Mode	Version	Connectivity	Del
BlrBranch1	60.95.197.129	6095197129-1234567890	CR50i	Route	9.4.2.0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
DelhiBranch1	220.220.220.220	220220220220-1234567890	CR50i	Route	9.4.2.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>
USHeadOffice	100.100.100.100	100100100100-1234567890	CR100i	Route	9.4.2.0	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Select All ☐

# User

User allows create and manage administrative user and role (permission).

Use to:

- [Create User](#)
- [Manage User](#)
- Create Role
- Manage Role

## Create User

Create administrative users to manage Cyberoam Central Console and devices. User cmcadmin is the default user who can configure and manage Cyberoam Central Console and all the devices and cannot be deleted.

Use to:

- [Create User](#)
- [Update administrator User details](#)

### To create administrative User

Prerequisite: Role created

1. Select **User → Create User**
2. Enter user name and password
3. Enter device description, if required
4. Select user role. Role defines the access level of the user. SuperUser is the default role which allows user to manage and configure Cyberoam Central Console as well as devices. Go to User>Create Role to define a new role.
5. Click Add to create user

Create User	
<b>User Information</b>	
User Name*	<input type="text"/>
Password*	<input type="password"/>
Description	<input type="text"/>
Select Role*	SuperUser ▼
<input type="button" value="Add"/> <input type="button" value="Cancel"/>	

## To update administrative User details

1. Select **User → Manage User** to view the list administrator user and click the username whose details is to be updated
2. Displays user name and password, modify if required
3. Displays user role, modify if required. Role defines the access level of the user. SuperUser is the default role which allows user to manage and configure Cyberoam Central Console as well as devices. Go to User>Create Role to define a new role.
4. Click Update to save the user details

The screenshot shows the 'Manage Users' interface. A table lists users: 'admin' (Description: This is superuser), 'admin\_a', and 'admin\_b'. A hand icon points to 'admin\_a'. An 'Edit User' modal is open, showing 'User Information' for 'admin\_a'. The 'User Name' field contains 'admin\_a', 'Password' is masked with dots, 'Description' is empty, and 'Select Role' is set to 'SuperUser'. 'Update' and 'Cancel' buttons are at the bottom.

User Name	Description
admin	This is superuser
admin_a	
admin_b	

### Edit User

**User Information**

User Name\*

Password\*

Description

Select Role\* SuperUser

## Manage User

Use to:

- [Update administrative User](#)
- [Delete administrative User](#)

## To delete administrative User

1. Select **User → Manage User** to view the list of users created
2. Click Del against the user to be deleted OR click Select All to delete all the users
3. Click Delete

Default user admin cannot be deleted.

The screenshot shows the 'Manage Users' interface with a table of users. The 'Del' column has checkboxes for 'admin' (disabled), 'admin\_a', and 'admin\_b' (checked). A 'Select All' checkbox is also present. A 'Delete' button is at the bottom right.

User Name	Description	Del
admin	This is superuser	<input type="checkbox"/>
admin_a		<input type="checkbox"/>
admin_b		<input checked="" type="checkbox"/>

Select All ☐

## Create Role

Use to:

- [Create new role](#)
- [Update role](#)

Roles define the access level of the user i.e. the administrator profile and local permission defines the role permission.

Role and local permission together determines the user's access to the various features of Cyberoam Central Console.

SuperUser is the default role which allows user to manage and configure Cyberoam Central Console as well as all the devices.

### To create new Role

1. Select **User → Create Role**
2. Enter role name
3. Enter description
4. Click Select to against Select Devices and Groups. It displays group wise devices that can be managed from Cyberoam Central Console. Click against Group name or Device name to enable. User to whom this role is assigned will be able to manage the enabled group/devices.
5. Enable Local permission to allow the configuration and management of Cyberoam Central Console.
6. Group list and device list displays the list of groups and devices which the user with this role can manage.
7. Click Add to create role

**Create Role**

**Role Information**

Role Name\*

Description

Select Devices or Groups\*  ☐ Local Permission

Selected Group List

Selected Device List

### To update Role

1. Select **User → Manage Role**
2. Displays role name, modify if required
3. Displays description, modify if required
4. Click Select to against Select Devices and Groups. It displays group wise devices that can be managed from Cyberoam Central Console. Click against Group name or Device name to enable. User to whom this role is assigned will be able to manage the enabled group/devices.

- Modify if required.
5. Enable Local permission to allow the configuration and management of Cyberoam Central Console. Modify if required.
  6. Group list and device list displays the list of groups and devices which the user with this role can manage.
  7. Click Update to save details.

Role Name	Description	Local Permission
SuperUser	This role is for Super User	Yes
block_1		Yes
block_2		No

### Edit Role

**Role Information**

Role Name\*: block\_2

Description:

Select Devices or Groups\*:  ☐ Local Permission

Selected Group List: General,

Selected Device List:

## Manage Role

Use to:

- [Update role](#)
- [Delete role](#)

### To delete Role

1. Select **User** → **Manage Role** to view the different roles created
2. Click Del against the role to be deleted OR click Select All to role all the users
3. Click Delete

Default role SuperUser cannot be deleted.

Role which is assigned to a user cannot be deleted.

Role Name	Description	Local Permission	Del
SuperUser	This role is for Super User	Yes	<input type="checkbox"/>
block_1		Yes	<input checked="" type="checkbox"/>
block_2		No	<input type="checkbox"/>

Select All ☐

# Firewall

A firewall protects the network from unauthorized access and typically guards the LAN and DMZ networks against malicious access; however, firewalls may also be configured to limit the access to harmful sites for LAN users.

The responsibility of firewall is to grant access from Internet to DMZ or Service Network according to the Rules and Policies configured. It also keeps watch on state of connection and denies any traffic that is out of connection state.

Firewall rules control traffic passing through the Cyberoam. Depending on the instruction in the rule, Cyberoam decides on how to process the access request. When Cyberoam receives the request, it checks for the source address, destination address and the services and tries to match with the firewall rule. If Identity match is also specified then firewall will search in the Live Users Connections for the Identity check. If Identity (User) found in the Live User Connections and all other matching criteria fulfills then action specified in the rule will be applied. Action can be allow or deny.

If Action is 'Allow' then each rule can be further configured to apply source or destination NATting (Network Address Translation). You can also apply different protection settings to the traffic controlled by firewall:

- Enable load balancing between multiple links
- Configure antivirus protection and spam filtering for SMTP, IMAP, POP3, and HTTP traffic. To apply antivirus protection and spam filtering, you need to subscribe for Gateway Anti Virus and Gateway Anti Spam modules individually. Refer to Licensing section for details.
- Implement Intrusion detection and prevention. To apply IDP policy you need to subscribe for Intrusion Detection and Prevention module. Refer to Licensing section for details.
- Configure content filtering policies. To apply content filtering you need to subscribe for Web and Application Filter module. Refer to Licensing section for details.
- Apply bandwidth policy restriction

By default, Cyberoam blocks any traffic to LAN.

- [Default Firewall Rules](#)
- [Create Firewall Rule](#)
- [Manage Firewall Rule](#)
- [DoS Settings](#)
- [DoS Bypass rule](#)

## Default Firewall rules

At the time of deployment, Cyberoam allows to define one of the following Internet Access policies using Network Configuration Wizard:

- Monitor only
- General Internet policy
- Strict Internet policy

Depending on the Internet Access policy set through Network Configuration Wizard, Cyberoam

defines the two default firewall rules as follows:

**Monitor only (Cyberoam applies the firewall rules in the order as specified below)**

1. Masquerade and Allow entire LAN to WAN traffic for all the authenticated users after applying following policies:
  - Internet Access policy – User specific
  - Bandwidth policy – User specific
  - Anti Virus & Anti Spam policy – Allows SMTP, POP3, IMAP and HTTP traffic without scanning
2. Masquerade and Allow entire LAN to WAN traffic for all the users without scanning SMTP, POP3, IMAP and HTTP traffic

**General Internet policy (Cyberoam applies the firewall rules in the order as specified below)**

1. Masquerade and Allow entire LAN to WAN traffic for all the authenticated users after applying following policies:
  - Internet Access policy – User specific
  - Bandwidth policy – User specific
  - Anti Virus & Anti Spam policy - Scan SMTP, POP3, IMAP and HTTP traffic
2. Masquerade and Allow entire LAN to WAN traffic for all the users after applying following policies:
  - Internet Access policy – Applies 'General Corporate Policy' to block Porn, Nudity, AdultContent, URL TranslationSites, Drugs, CrimeandSuicide, Gambling, MilitancyandExtremist, PhishingandFraud, Violence, Weapons categories
  - IDP – General policy
  - Anti Virus & Anti Spam policy - Scan SMTP, POP3, IMAP and HTTP traffic

**Strict Internet policy (Cyberoam applies the firewall rules in the order as specified below)**

1. Masquerade and Allow entire LAN to WAN traffic for all the authenticated users after applying following policies:
  - Internet Access policy – User specific
  - Bandwidth policy – User specific
  - IDP – General policy
  - Anti Virus & Anti Spam policy - Scan SMTP, POP3, IMAP and HTTP traffic
2. Drop entire LAN to WAN traffic for all the users



**Default Firewall rules can be modified as per the requirement but cannot be deleted**

**IDP policy will not be effective until Intrusion Detection and Prevention (IDP) module is subscribed**

**Virus and Spam policy will not be effective until Gateway Anti Virus and Gateway Anti-spam modules are subscribed respectively**

**If Internet Access Policy is not set through Network Configuration Wizard at the time of deployment, the entire traffic is dropped**

Additional firewall rules can be defined to extend or override the default rules. For example, rules can be created that block certain types of traffic such as FTP from the LAN to the WAN, or allow certain types of traffic from specific WAN hosts to specific LAN hosts, or restrict use of certain

protocols such as Telnet to authorized users on the LAN.

Custom rules evaluate network traffic source IP addresses, destination IP addresses, User, IP protocol types, and compare the information to access rules created on the Cyberoam appliance. Custom rules take precedence, and override the default Cyberoam firewall rules.

## Create Firewall Rule

Use to

- [Create firewall rule](#)
- [Update firewall rule](#)

Previous versions allowed creating firewall rules based on source and destination IP addresses and services but now Cyberoam's Identity based firewall allows to create firewall rules embedding user identity into the firewall rule matching criteria.

Firewall rule matching criteria now includes:

- Source and Destination Zone and Host
- User
- Service

Following Unified Threat Control policies can be attached to the firewall rule as per the defined matching criteria:

- Intrusion Detection and Prevention (IDP)
- Internet Access
- Bandwidth Management

To create a firewall rule, you should:

- Define matching criteria
- Associate action to the matching criteria
- Attach the threat management policies

For example, now you can:

- Restrict the bandwidth usage to 256kb for the user John every time he logs on from the IP 192.168.2.22
- Restrict the bandwidth usage to 1024kb for the user Mac if he logs on in working hours from the IP 192.168.2.22

Processing of firewall rules is top downwards and the first suitable rule found is applied.

Hence, while adding multiple rules, it is necessary to put specific rules before general rules. Otherwise, a general rule might allow a packet that you specifically have a rule written to deny later in the list. When a packet matches the rule, the packet is immediately dropped or forwarded without being tested by the rest of the rules in the list.



## To create firewall rule

1. Select **Firewall → Create Rule**
2. Select Group ID. After successful creation, Firewall rule can be applied to any or all the devices in the selected group.
3. Specify source zone and host IP address/network address to which the rule applies.
4. To define host group based firewall rule you need to define host group.
5. Under Select Address, click Create Host Group to define host group from firewall rule itself or from **Firewall → Host Group → Create**

Under Select Address, click Add Host to define host group from firewall rule itself rule itself or from **Firewall → Host → Add Host**

6. Click Enable to check the user identity. (Only if source zone is LAN/DMZ)  
Check identity allows you to check whether the specified user/user group from the selected zone is allowed the access of the selected service or not.

Enable check identity to limit access to available services and apply following policies per user:

- Internet Access policy for Content Filtering (User's Internet Access policy will be applied automatically but will not be effective till the Web and Content Filtering module is subscribed)
  - Schedule Access
  - IDP (User's IDP policy will be applied automatically but will not be effective till the IDP module is subscribed)
  - Anti Virus scanning (User's anti virus policy will be applied automatically but it will not be effective till the Gateway Anti Virus module is subscribed)
  - Anti Spam scanning (User's anti spam policy will be applied automatically but it will not be effective till the Gateway Anti Spam module is subscribed)
  - Bandwidth policy - User's bandwidth policy will be applied automatically
  - The policy selected in Route through Gateway is the static routing policy that is applicable only if more than one gateway is defined and used for load balancing.
7. Specify destination zone and host IP address /network address to which the rule applies.
  8. To define host group based firewall rule you need to define host group.

Under Select Address, click Create Host Group to define host group from firewall rule itself or from **Firewall → Host Group → Create**

Under Select Address, click Add Host to define host group from firewall rule itself rule itself or from **Firewall → Host → Add Host**

9. Select service/service group to which the rule applies.  
Services represent types of Internet data transmitted via particular protocols or applications.

Protect by configuring rules to

- block services at specific zone
- limit some or all users from accessing certain services
- allow only specific user to communicate using specific service

Under Select Here, click Create Service Group to define service group from firewall rule itself rule itself or from **Firewall → Service → Create Service**

Cyberoam provides several standard services and allows creating the custom services also. Under Select Here, click Create Service to define service from firewall rule itself rule itself or from **Firewall → Service → Create Service**

10. Select Schedule for the rule
11. Select rule action
  - Accept – Allow access
  - Drop – Silently discard i.e. without sending 'ICMP port unreachable' message to the source
  - Reject – Deny access and send 'ICMP port unreachable' message to the source
12. Click Apply Source NAT and select the SNAT policy to be applied (Only if Action is 'ACCEPT')  
It allows access but after changing source IP address i.e. source IP address is substituted by the IP address specified in the SNAT policy.

You can create SNAT policy from firewall rule itself or from **Firewall → SNAT Policy → Create**



**This option is not available if Cyberoam is deployed as Bridge**

13. Click Advanced Settings to apply different protection settings to the traffic controlled by firewall. You can:
  - Enable load balancing and failover when multiple links are configured
  - Configure antivirus protection and spam filtering for SMTP, IMAP, POP3, and HTTP policies.
  - Implement Intrusion detection and prevention.
  - Configure content filtering policies.
  - Apply bandwidth policy
14. Select DNAT policy to be applied  
DNAT rule tells the firewall to forward the requests from the specified machine and port to the specified machine and port.

Under Select Here, click Create DNAT Policy to define dn timer policy from firewall rule itself rule itself or from **Firewall → DNAT Policy → Create**



**This option is not available if Cyberoam is deployed as Bridge**

15. Select IDP policy for the rule. Refer to IDP, Policy for details on creating IDP policy.



**IDP policy will be applicable only for those Cyberoam Appliances for whom Intrusion Detection and Prevention add-on module is subscribed.**

16. Select Internet access policy for the rule. It can be applied to LAN to WAN rule only.  
Internet Access policy controls web access. Refer to Policies, Internet Access Policy for details on creating Internet Access policy.



**Content filtering will be applicable only for those Cyberoam Appliances for whom Web and Application Filter add-on module is subscribed.**

17. Select Bandwidth policy for the rule  
Only Firewall rule based Bandwidth policy can be applied. Bandwidth policy allocates & limits the maximum bandwidth usage of the user. Refer to Policies, Bandwidth Policy for details on creating Bandwidth policy.

18. Click the protocol for which the virus and spam scanning is to be enabled  
By default, HTTP scanning is enabled.

If Check Identity is enabled, the policy will be applied to the specified user/user group only.



**Antivirus protection and spam filtering will be applicable only for those Cyberoam Appliances for whom Gateway Anti Virus and Gateway Anti Spam modules are individually subscribed.**


19. Click Log Traffic to enable/disable traffic logging for the rule. Make sure, firewall rule logging in ON/Enable from the Logging Management. Refer to Cyberoam Console Guide, Cyberoam Management for more details.

To log the traffic permitted and denied by the firewall rule, you need to ON/Enable the firewall rule logging from the Web Admin Console→Firewall rule and from the Telnet Console→Cyberoam Management.

20. Specify full description of the rule  
21. Click create to create the rule

Create Firewall Rule		Register	CCC	Help	Logout
<b>Matching Criteria</b>					
Group Id	General				
Source *	Select Zone	Select Address			
<input type="checkbox"/> Check Identity					
Destination*	Select Zone	Select Address			
Service/Service Group*	Select Here				
Apply Schedule	All the Time				
<b>Firewall Action When Criteria Match</b>					
Action*	Select Here				
<input type="checkbox"/> Apply Source NAT	MASQ				
<input checked="" type="checkbox"/> <b>Advanced Settings (Destination NAT, IDP Policy, Internet Access Policy, Bandwidth Policy, Anti-Virus and Anti-Spam Settings, Log Traffic)</b>					
<b>Policies</b>					
IDP Policy	Select Here				
Internet Access Policy	Select Here				
Bandwidth Policy	Select Here				
<b>Anti-Virus &amp; Anti-Spam Settings</b>					
Scan Protocol(s)	<input type="checkbox"/> SMTP <input type="checkbox"/> POP3 <input type="checkbox"/> IMAP <input type="checkbox"/> FTP <input type="checkbox"/> HTTP				
<b>Log Traffic</b>					
Log Traffic	<input type="checkbox"/> Enable				
<b>Description</b>					
Description	<input type="text"/>				
<div> <div>Create</div> <div>Cancel</div> </div>					

## To update firewall rule

1. Select **Firewall → Manage Rule** and select the Device Group. List of firewall rules created for the selected group will be displayed. click Edit icon  against the rule to be modified.
2. Displays source zone and host IP address/network address to which the rule applies. Modify host IP address/network address, if required.
3. To define host group based firewall rule you need to define host group. Under Select Address, click Create Host Group to define host group from firewall rule itself or from **Firewall → Host Group → Create**

Under Select Address, click Add Host to define host group from firewall rule itself rule itself or from **Firewall → Host → Add Host**

4. Click Enable to check the user identity. (Only if source zone is LAN/DMZ)  
Check identity allows you to check whether the specified user/user group from the selected zone is allowed the access of the selected service or not.

Enable check identity to limit access to available services and apply following policies per user:

- Internet Access policy for Content Filtering (User's Internet Access policy will be applied automatically but will not be effective till the Web and Content Filtering module is subscribed)
  - Schedule Access
  - IDP (User's IDP policy will be applied automatically but will not be effective till the IDP module is subscribed)
  - Anti Virus scanning (User's anti virus policy will be applied automatically but it will not be effective till the Gateway Anti Virus module is subscribed)
  - Anti Spam scanning (User's anti spam policy will be applied automatically but it will not be effective till the Gateway Anti Spam module is subscribed)
  - Bandwidth policy - User's bandwidth policy will be applied automatically
  - The policy selected in Route through Gateway is the static routing policy that is applicable only if more than one gateway is defined and used for load balancing.
5. Displays destination zone and host IP address /network address to which the rule applies.
  6. Modify host IP address/network address, if required.

To define host group based firewall rule you need to define host group.

Under Select Address, click Create Host Group to define host group from firewall rule itself or from **Firewall → Host Group → Create**

Under Select Address, click Add Host to define host group from firewall rule itself rule itself or from **Firewall → Host → Add Host**

7. Displays service/service group applied to the rule modify if required.  
Services represent types of Internet data transmitted via particular protocols or applications.

Protect by configuring rules to

- block services at specific zone
- limit some or all users from accessing certain services
- allow only specific user to communicate using specific service

Under Select Here, click Create Service Group to define service group from firewall rule itself rule itself or from **Firewall → Service → Create Service**

Cyberoam provides several standard services and allows creating the custom services also. Under Select Here, click Create Service to define service from firewall rule itself rule itself or from **Firewall → Service → Create Service**

8. Displays schedule applied to the rule, modify if required
9. Displays rule action, modify if required

Accept – Allow access

Drop – Silently discard i.e. without sending 'ICMP port unreachable' message to the source

Reject – Deny access and send 'ICMP port unreachable' message to the source

10. Click Apply Source NAT and select the SNAT policy to be applied (Only if Action is 'ACCEPT')  
It allows access but after changing source IP address i.e. source IP address is substituted by the IP address specified in the SNAT policy.

You can create SNAT policy from firewall rule itself or from **Firewall → SNAT Policy → Create**



**This option is not available if Cyberoam is deployed as Bridge**

11. Click Advanced Settings to apply different protection settings to the traffic controlled by firewall. You can:
  - Enable load balancing and failover when multiple links are configured
  - Configure antivirus protection and spam filtering for SMTP, IMAP, POP3, and HTTP policies.
  - Implement Intrusion detection and prevention.
  - Configure content filtering policies.
  - Apply bandwidth policy
12. Displays DNAT policy applied to the rule, modify if required  
DNAT rule tells the firewall to forward the requests from the specified machine and port to the specified machine and port.

Under Select Here, click Create DNAT Policy to define dn timer policy from firewall rule itself rule itself or from **Firewall → DNAT Policy → Create**



**This option is not available if Cyberoam is deployed as Birdge**

13. Displays IDP policy applied to the rule, modify if required. Refer to IDP, Policy for details on creating IDP policy.



**IDP policy will be applicable only for those Cyberoam Appliances for whom Intrusion Detection and Prevention add-on module is subscribed.**

14. Displays Internet access policy applied to the rule, modify if required. It can be applied to LAN to WAN rule only.  
Internet Access policy controls web access. Refer to Policies, Internet Access Policy for details on creating Internet Access policy.



**Content filtering will be applicable only for those Cyberoam Appliances for whom Web and Application Filter add-on module is subscribed.**

15. Displays Bandwidth policy applied to the rule, modify if required.

Only Firewall rule based Bandwidth policy can be applied. Bandwidth policy allocates & limits the maximum bandwidth usage of the user. Refer to Policies, Bandwidth Policy for details on creating Bandwidth policy.

16. Click the protocol for which the virus and spam scanning is to be enabled

By default, HTTP scanning is enabled.



**Antivirus protection and spam filtering will be applicable only for those Cyberoam Appliances for whom Gateway Anti Virus and Gateway Anti Spam modules are individually subscribed.**

17. Click Log Traffic to enable/disable traffic logging for the rule. Make sure, firewall rule logging is ON/Enable from the Logging Management. Refer to Cyberoam Console Guide, Cyberoam Management for more details.

To log the traffic permitted and denied by the firewall rule, you need to ON/Enable the firewall rule logging from the Web Admin Console→Firewall rule and from the Telnet Console→Cyberoam Management. Specify full description of the rule

18. Displays full description of the rule, modify if required  
19. Click Save to save the rule

Manage Firewall Rules

Register CCC Help Logout

Select Device Group

General

Insert Rule

Select Columns

ID	Enable	Source	Identity	Destination	Service	Action	SNAT Policy	IAP	Manage	Apply
LAN - WAN (2 Rules)										
2	<input checked="" type="checkbox"/>	Any Host	Any Live User	Any Host	All Services	Accept	MASQ	User's Pol...		
1	<input checked="" type="checkbox"/>	Any Host	-	Any Host	All Services	Accept	MASQ	Allow All		

Edit Firewall Rule

Register CCC Help Logout

Matching Criteria

Group Id

General

Source \*

LAN

Any Host

☒ Check Identity

Any Live User

Destination \*

WAN

Any Host

Service/Service Group\*

All Services

Apply Schedule

All the Time

Firewall Action When Criteria Match

Action\*

Accept

☒ Apply Source NAT

MASQ

☒ Advanced Settings (Destination NAT, IDP Policy, Internet Access Policy, Bandwidth Policy, Anti-Virus and Anti-Spam Settings, Log Traffic)

Policies

IDP Policy

Select Here

Internet Access Policy

Select Here

Bandwidth Policy

Select Here

Anti-Virus & Anti-Spam Settings

Scan Protocol(s)

☐ SMTP
☐ POP3
☐ IMAP
☐ FTP
☒ HTTP

Log Traffic

Log Traffic

☐ Enable

Description

Description

Save

Cancel

## Manage Firewall Rules

Use to:


- Update rule
- Deactivate rule
- Delete rule. Deleting firewall rule will delete firewall rule from Cyberoam Central Console and not from the devices.
- [Append rule](#)
- [Customize the screen display](#)

### Manage firewall rule screen components

Select Firewall → Manage Rule to view the list of rules


Append Rule button - Click to add zone to zone rule


Select Column button – Click to customize the number of columns to be displayed on the page


Enable/Disable rule icon  - Click to activate/deactivate the rule. If you do not want to apply the firewall rule temporarily, disable rule instead of deleting.


Green – Active Rule


Red – Deactive Rule

Edit icon  - Click to edit the rule. Refer to Update Firewall rule for more details.

Insert icon  - Click to insert a new rule before the existing rule. Refer to Create Firewall Rule for more details.

Delete icon  - Click to delete the rule. Deleting firewall rule will delete firewall rule from Cyberoam Central Console and not from the devices. To delete firewall rule from the device, use Remove function.

Apply button  - Click to apply firewall rule to all the selected devices in the selected Group.

Remove button  - Click to remove firewall rule from all the selected devices in the selected Group.

Manage Firewall Rules

CCC

Help

Logout

Group Name

General

Insert Rule

Select Columns

ID	Enable	Source	Identity	Destination	Service	Action	SNAT Policy	IAP	Manage	Apply
LAN - WAN (2 Rules)										
2		Any Host	Any Live User	Any Host	All Services	Accept	MASQ	User's Pol...		<div>Apply</div> <div>Remove</div>
1		Any Host	-	Any Host	All Services	Accept	MASQ	Allow All		<div>Apply</div> <div>Remove</div>

### To append rule

Append Rule adds the new rule above the default rules if zone-to-zone rule set exists else appends new rule as new zone-to-zone rule set in the end.

Select Firewall → Manage Firewall

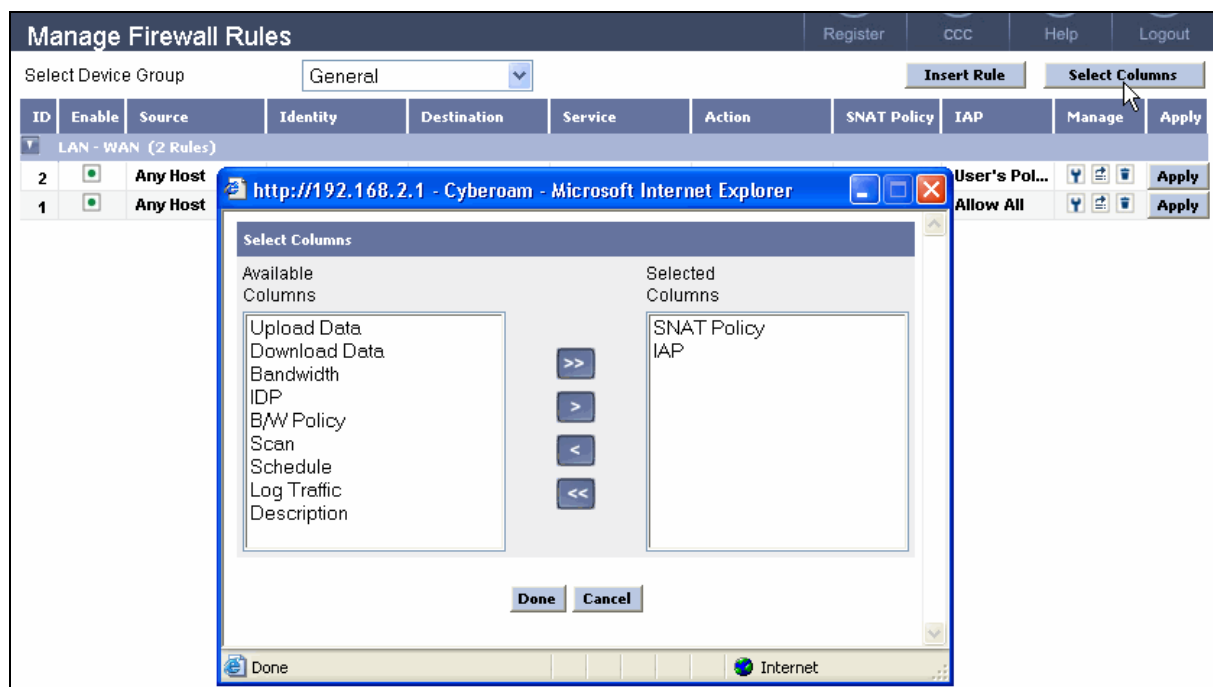
Click Append rule to open the create firewall rule page.

Refer to Define Firewall Rule for more details.

## To customize Screen Display

By default, Manage Firewall Rules page displays details of the rule in the following eight columns: ID, Enable, Source, Identity, Destination, Service, Action, and Manage. You can customize the number of columns to be displayed as per your requirement.

1. Select **Firewall → Manage Firewall** to open the manage page
2. Click Select Columns
3. It opens the new window. 'Available Columns' list displays the columns that can be displayed on the page.
4. Click the required column and use Right arrow button to move the selected column to the 'Selected Columns' list
5. Click Done





## Host

Use to:

- [Add Host](#)
- [Manage Host](#)

Firewall rule can be created for the individual host or host groups. By default, the numbers of hosts equal to the ports in the appliance are already created.

## Add Host

1. Select **Firewall → Host → Add**
2. Enter host name
3. Select host type i.e. single IP address with subnet or range of IP addresses
4. Select host group
5. Create to add a new host

## Manage Host

Use to:

- Assign host to Device (Cyberoam Appliance)
- Delete host. Deleting host will delete host from the Cyberoam Central Console and not from the devices.

### To assign Host to a Device

1. Select **Firewall → Host → Manage**
2. Click Apply against the host name. It opens a new page and displays group wise devices. Enable the check box against the group or device to which the host is to be added.
3. Click Apply. Applied will be displayed against the group/device, if the host is added successfully.

**Manage Host** ccc Help Logout

Host Name	Address/Range	Host Group	Apply	Del
mailserver	[REDACTED]		Apply	<input type="checkbox"/>
webserver	[REDACTED]		Apply	<input type="checkbox"/>
databaseserver	[REDACTED]		Apply	<input type="checkbox"/>
intranetserver	[REDACTED]		Apply	<input type="checkbox"/>
admin1			Apply	<input type="checkbox"/>
admin2			Apply	<input type="checkbox"/>
voipdevice1			Apply	<input type="checkbox"/>
voipdevice2			Apply	<input type="checkbox"/>
voipdevice3			Apply	<input type="checkbox"/>
traininghost			Apply	<input type="checkbox"/>
cccmanage			Apply	<input type="checkbox"/>
			Select All	<input type="checkbox"/>
			<b>Delete</b>	

http://[REDACTED]/cmc/webpages/cmc/DeviceGroupTree.js...

**Select Device**

- ☐ **General**
  - ☐ StandbyUnit ([REDACTED])
- ☐ **USBranches**
  - ☐ USBranch1 ([REDACTED])
  - ☐ USBranch2 ([REDACTED])
- ☐ **INBranches**
  - ☐ BlrBranch1 ([REDACTED])
  - ☐ DelhiBranch1 ([REDACTED])
- ☐ **HeadOffices**
  - ☐ USHeadOffice ([REDACTED]) Not Connected
  - ☐ INHeadOffice ([REDACTED])

**Apply** **Close**

### To delete host

1. Select **Firewall → Host → Manage**
2. Click Del against the host to be deleted OR click Select All to delete all the hosts
3. Click Delete

**Manage Host** ccc Help Logout

Host Name	Address/Range	Host Group	Apply	Del
mailserver	[REDACTED]		Apply	<input checked="" type="checkbox"/>
webserver	[REDACTED]		Apply	<input checked="" type="checkbox"/>
databaseserver	[REDACTED]		Apply	<input type="checkbox"/>
intranetserver	[REDACTED]		Apply	<input type="checkbox"/>
			Select All	<input type="checkbox"/>
			<b>Delete</b>	

## Host Group

Use to:

- Create Host group
- Manage Host group

Host group is the grouping on hosts.

### Create Host Group

1. Select **Firewall → Host Group → Create**
2. Enter host group name
3. Enter description for the group
4. Click Create to create the group. If the Group is successfully created, you can add the hosts to the group. Refer to Add Host to Host Group for details.

### Manage Host Group

Use to:

- View host group details
- Assign Host group to a Device
- Add/Delete host from host group
- Delete host group. Deleting host group will delete host group from the Cyberoam Central Console and not from the devices.

### To add Host to Host Group

1. Click Add if adding host at the time of creation of the Host Group OR Select **Firewall → Host Group → Manage** to view the list of groups created.
2. Click host group to which host is to be added. Host Group details is displayed.
3. Click Add. List of hosts that can be added to the group is displayed.
4. Click against the host to be added
5. Click Add

**Manage Host Group**

Host Group Name	Description	Apply	Del
DMZservers		Apply	<input type="checkbox"/>

**Edit Host Group**

Host Group Name\* DMZservers

Description

List Of Hosts

Host Name	Address/Range
No Host added.	

Add

Save Cancel

### To assign Host Group to a Device

1. Select **Firewall → Host Group → Manage**
2. Click Apply against the host name. It open as a new page and displays group wise devices. Enable the check box against the group or device to which the host group is to be added.
3. Click Apply. Applied will be displayed against the group/device, if the host group is added successfully.

**Manage Host Group**

Host Group Name	Description	Apply
DMZservers		Apply
admindevices1		Apply
VoipDevices		Apply

**Select Device**

- ☐ General
  - ☐ StandbyUnit (1)
- ☐ USBranches
  - ☐ USBranch1 (1)
  - ☐ USBranch2 (1)
- ☐ INBranches
  - ☐ BlrBranch1 (8)
  - ☐ DelhiBranch1 (2)
- ☐ HeadOffices
  - ☐ USHeadOffice (1)
  - ☐ INHeadOffice (1)

Apply Close

### To delete Host from Host Group

1. Select **Firewall → Host Group → Manage** to view the list of groups created.
2. Click host group from which the host is to be deleted.
3. Click Del against the hosts to be deleted when the list of hosts that can be added to the group is displayed.
4. Click Delete

### To delete Host Group

1. Select **Firewall → Host Group → Manage** to view the list of groups created.
2. Click Del against the groups to be deleted
3. Click Delete

Deleting host group will delete host group from the Cyberoam Central Console and not from the devices.

Manage Host Group				CCC	Help	Logout
Host Group Name	Description	Apply	Del			
<u>DMZservers</u>		<input type="button" value="Apply"/>	<input checked="" type="checkbox"/>			
<u>admindevices1</u>		<input type="button" value="Apply"/>	<input type="checkbox"/>			
<u>VoipDevices</u>		<input type="button" value="Apply"/>	<input type="checkbox"/>			
			Select All <input type="checkbox"/>			
			<input type="button" value="Delete"/>			

## Services

Services represent types of Internet data transmitted via particular protocols or applications.

Protect your network by configuring firewall rules to

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

Cyberoam provides several standard services and allows creating:

- Customized service definitions
- Firewall rule for customized service definitions

### Create Service

Use to:

- [Create Service](#)
- [Update Service](#) .To edit service details, click the service name to be modified.

#### To create service

1. Select **Firewall → Services → Create**
2. Enter service name
3. Select type of protocol  
For IP - Select Protocol No.  
For TCP - Enter Source and Destination port  
For UDP - Enter Source and Destination port  
For ICMP - Select ICMP Type and Code
4. Enter Description
5. Click Create to create and save the details. If service is created successfully, click Add to add protocol details. Refer to Add Protocol details for more details.

**Create Service** Register

**Create Service**

Service Name\*

Select Protocol\* TCP

Source Port\*  (1:65535)

Destination Port\*  (1:65535)

Description

Create Cancel

## To update service

1. Select **Firewall → Services → Manage**
2. Enter service name
3. Select type of protocol
  - For IP - Select Protocol No.
  - For TCP - Enter Source and Destination port
  - For UDP - Enter Source and Destination port
  - For ICMP - Select ICMP Type and Code
4. Enter Description
5. Click Create to create and save the details. If service is created successfully, click Add to add protocol details. Refer to Add Protocol details for more details.

**Manage Service**

Service Name	Details	Description	Apply	Del
trainingservice	TCP (1:65535) / (3389)		Apply	<input type="checkbox"/>
All Services	All Services	All Services	-	<input type="checkbox"/>

**Edit Service**

Service Name\* trainingservice

Description

**Protocol Details**

Protocol	Details	Del
TCP	source port (1:65535)/ destination port (3389)	<input type="checkbox"/>

Add Delete

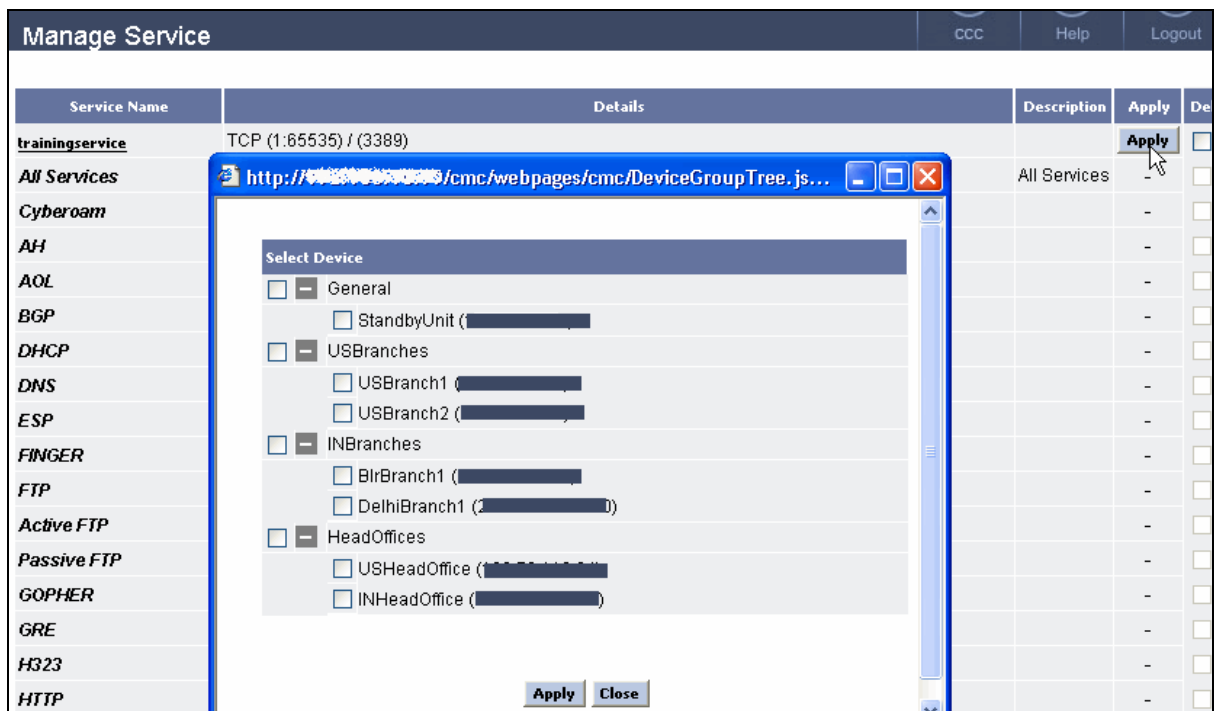
## Manage Service

Use to:

- View Service details
- [Update Service](#). To edit service details, click the service name to be modified.
- Assign Service to a Device
- Add Protocol details
- Delete Protocol details
- Delete Service. Deleting service will delete service from the Cyberoam Central Console and not from the devices.

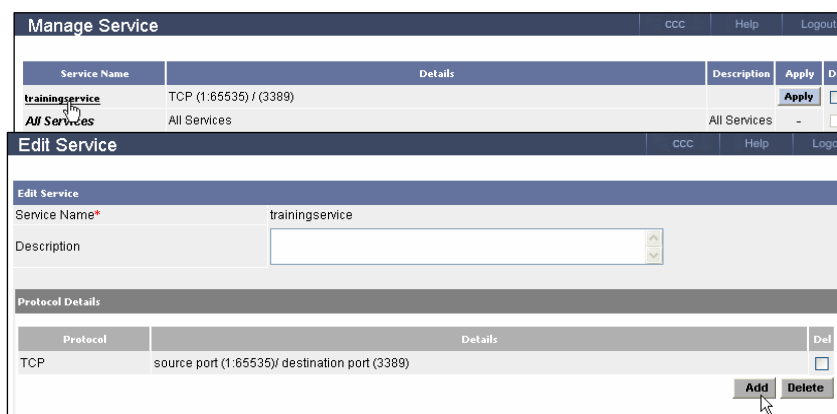
## To assign Service to a Device

1. Select **Firewall → Service → Manage**
2. Click Apply against the Service name. It open as a new page and displays group wise devices. Enable the check box against the group or device to which the Service is to be added.
3. Click Apply. Applied will be displayed against the group/device, if the Service is added successfully.



### To add protocol details

1. Click Add if adding details at the time of creation of the Service OR Select **Firewall** → **Services** → **Manage** to view the list of service and click the service to which details are to be added
2. Click Add
3. Select type of protocol  
 For IP - Select Protocol No.  
 For TCP - Enter Source and Destination port  
 For UDP - Enter Source and Destination port  
 For ICMP - Select ICMP Type and Code
4. Click Add





## To delete protocol details

1. Select **Firewall → Services → Manage** to view the list of service and click the service from which the details are to be deleted
2. Click Del against the details to be deleted OR click Select All to select all the protocol details
3. Click Delete to delete the selected details

## To delete Service

1. Select **Firewall → Services → Manage** to view the list of service
2. Click Dele against the services to be deleted or Select All to delete all the services
3. Click Delete to delete the selected services



**Default Services cannot be updated or deleted**

Deleting service will delete service from the Cyberoam Central Console and not from the devices.

Manage Service					ccc	Help	Logout
Service Name	Details	Description	Apply	Del			
<u>trainingservice</u>	TCP (1:65535) / (3389)		<b>Apply</b>	<input checked="" type="checkbox"/>			
<b>All Services</b>	All Services	All Services	-	<input type="checkbox"/>			
<b>Cyberoam</b>	UDP (1024:65535) / (6060)		-	<input type="checkbox"/>			
<b>AH</b>	IP Protocol No 51 (IPv6-Auth)		-	<input type="checkbox"/>			
<b>AOL</b>	TCP (1:65535) / (5190:5194)		-	<input type="checkbox"/>			
<b>BGP</b>	TCP (1:65535) / (179)		-	<input type="checkbox"/>			
<b>HA Service</b>	TCP (1:65535) / (273), UDP (1:65535) / (694), TCP (1:65535) / (22)		-	<input type="checkbox"/>			
				Select All			
				<input type="checkbox"/>			
				<b>Delete</b>			

# Categories

Cyberoam's content filtering capabilities prevent Internet users from accessing non-productive or objectionable websites that take valuable system resources from your network at the same time prevents hackers and viruses that can gain access to your network through their Internet connections.

Cyberoam lets you prevent Internet users from accessing URLs that contain content the company finds objectionable. Cyberoam's Categories Database contains categories covering Web page subject matter as diverse as adult material, astrology, games, job search, and weapons. It is organized into general categories, many of which contain collections of related Internet sites with specific content focus. In other words, database is a collection of site/host names that are assigned a category based on the major theme or content of the site.

Categories Database consists of three types of categories:

Web Category – Grouping of Domains & Keywords

File Types – Grouping of File extensions

Application Protocol – Grouping of protocols

Apart from the default Categories provided by Cyberoam, custom category can be created and edited at any time. Adding category gives you increased flexibility in managing Internet access for your organization. Once a new category is created, it must be added to a policy so that Cyberoam knows when to enforce it and for which groups/users.

- [Web Category](#)
- [File Types Category](#)
- [Application Protocol Category](#)

## Web Category

Web category is the grouping of Domains and Keywords used for Internet site filtering. Domains and any URL containing the keywords defined in the Web category will be blocked.

Each category is grouped according to the type of sites in the category. Categories are grouped in to four types and specifies whether the surfing those categories is considered as productive or not:

- Neutral
- Productive
- Non-working
- Un-healthy

For your convenience, Cyberoam provides a database of default Web categories. You can use these or even create new web categories to suit your needs. To use the default web categories, the add-on module Web and Application Filter should be registered.

Depending on the organization requirement, allow or deny access to the categories with the help of policies by groups, individual user, time of day, and many other criteria.

Custom web category is given priority over default category while allowing/restricting the access.

- [Create Custom Web Category](#)
- [Manage Custom Web Category](#)
- [Manage Default Web Category](#)

### Create Custom Web category

Use to:

- Create custom web category
- Update custom web category

### To create custom web category

1. Select **Categories → Web Category → Create Custom**
2. Enter web category name



**Custom category name cannot be same Default category name.**

3. Enter relevant description
4. Select Category Type
5. Click Create/Update to save the details
6. Under Domain Management
  - Click Add to add domain. (See To add Domain)
  - To delete domain from category, see To delete Domain.
7. Under Keyword Management
  - Click Add to add keyword. (See To add Keyword)
  - To delete keyword from category, see To delete Keyword.

### Create Custom Web Category

**Create Custom Web Category**

Name\*

Description

Category Type Neutral

- Neutral
- Productive
- Non Working
- Neutral
- UnHealthy

**Create** **Cancel**

### Edit Custom Web Category

ccc Help Logout

**Web Category 'Delhcategory' has been created successfully**

**Update Custom Web Category**

Name\* Delhcategory

Description

Category Type Neutral

**Domain Management**

Add Domain

Domains\*

**Add** **Cancel**

**Keyword Management**

**Add**

Keywords **Select**

**Update** **Cancel**

### To update Custom Web category

1. Select **Categories** → **Web Category** → **Manage Custom** to view the list of custom web categories and click web category to be modified
2. Displays web category name which cannot be modified
3. Change the description, if required.
4. Under Domain Management
  - Click Add to add domain. (See To add Domain)
  - To delete domain from category, see To delete Domain.
5. Under Keyword Management
  - Click Add to add keyword. (See To add Keyword)
  - To delete keyword from category, see To delete Keyword.

- Click Update if any modifications are done

The screenshot displays two overlapping windows from the Cyberoam Central Console. The top window, titled 'Manage Custom Web Category', contains a table with columns: Category Name, Type, Description, Apply, and Del. It lists three categories: 'ccccustom' (Neutral), 'MyCompanySites' (Productive), and 'yahooWedMail' (Productive). The bottom window, titled 'Edit Custom Web Category', shows the 'Update Custom Web Category' form. The 'Name' field is set to 'MyCompanySites', the 'Description' field is empty, and the 'Category Type' is set to 'Productive'. Below the form are two sections: 'Domain Management' and 'Keyword Management'. The 'Domain Management' section has an 'Add' button and a table with columns 'Domains' and 'Select', listing domains like cyberoam.com, 24onlinebilling.com, crestel.in, and elitecore.com. The 'Keyword Management' section has an 'Add' button and a table with columns 'Keywords' and 'Select'.

### To add Domain

- Click Add under Domain Management if adding details at the time of creation of the Web category OR Select **Categories → Web Category → Manage Custom** and click category name to which domain is to be added, if adding after the creation of category
- Enter domain names. Multiple domain names can be specified using comma e.g. www.hotmail.com, www.yahoo.com
- Click Add to save



**Domains can be added at the time of creation of category or later whenever required**

### To add Keyword

- Click Add under Keyword Management if adding details at the time of creation of the Web category OR Select **Categories → Web Category → Manage Custom** and click category name to which domain is to be added, if adding after the creation of category
- Enter keywords. Multiple keywords can be specified using comma e.g. cricket, football, boxing
- Click Add to save



**Keywords can be added at the time of creation of category or later whenever required**

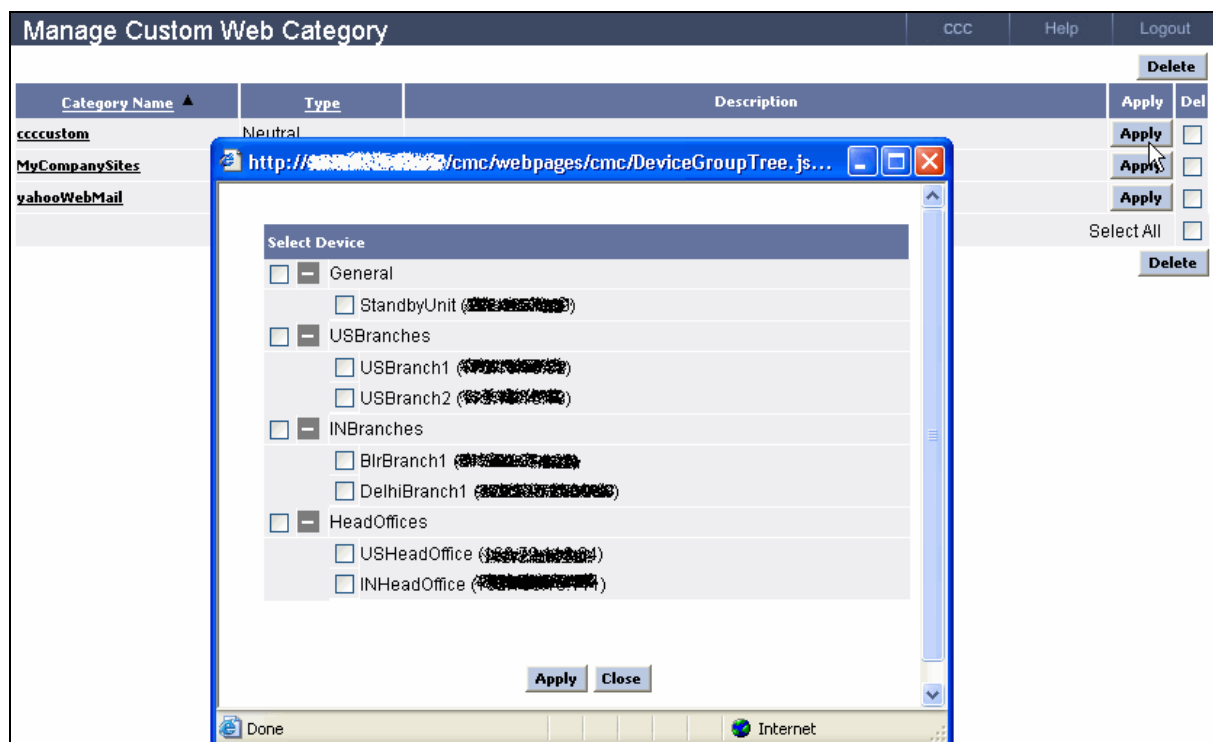
## Manage Custom Web category

Use to:

- Modify Description
- Add Domains to web category
- Delete Domains from web category
- Add Keywords to web category
- Assign to a Device
- Delete Keywords from web category
- Delete custom web category. Deleting custom web category will delete from the Cyberoam Central Console and not from the devices.

### To assign Web category to a Device

1. Select **Categories → Web Category → Manage Custom**
2. Click Apply against the Web category name. It opens a new page and displays group wise devices. Enable the check box against the group or device to which the Web category is to be added.
3. Click Apply. Applied will be displayed against the group/device, if the Web category is added successfully.



## To delete Domain

1. Select **Categories → Web Category → Manage Custom** to view the list of Web categories and click Web Category from which the domain is to be removed
2. Click Select against the domain(s) to be removed OR Click Select All to remove all the domains
3. Click Delete

## To delete Keyword

1. Select **Categories → Web Category → Manage Custom** to view the list of Web categories and click Web Category from which the keyword is to be removed
2. Click Select against the keyword(s) to be removed OR Click Select All to remove all the keywords
3. Click Delete

## To delete Web Category



**Not attached to any policy**

1. Select **Categories → Web Category → Manage Custom** to view the list of Web categories
2. Click Select against the web category to be removed OR Click Select All to remove all the web categories
3. Click Delete

Deleting custom web category will delete from the Cyberoam Central Console and not from the devices.

Manage Custom Web Category			CCC	Help	Logout
			Delete		
Category Name ▲	Type	Description	Apply	Del	
ccccustom	Neutral		Apply	<input checked="" type="checkbox"/>	
MyCompanySites	Productive		Apply	<input type="checkbox"/>	
yahooWebMail	Productive		Apply	<input type="checkbox"/>	
			Select All <input type="checkbox"/>		
			Delete		

## Manage Default Web category

Default Web categories are available for use only if 'Web and Application Filter' add-on module is registered. Database of web categories is constantly updated by Cyberoam.

Each category is grouped according to the type of sites in the category. Categories are grouped in to four types and specifies whether the surfing those categories is considered as productive or not:

- Neutral
- Productive
- Non-working
- Un-healthy



**Default web categories cannot be modified or deleted.**

**Custom web category is given priority over default category while allowing/restricting access.**

To view the list of default web categories, go to Categories → Web Category → Manage Default

Category Name	Type	Description
ActiveX	Non Working	Includes all ActiveX applications
AdultContent	UnHealthy	Adult sites not falling in "Porn, Nudity, Swimwear & Lingerie, Sex Education, and Sexual Health & Medicines" will be included in "Adult Content" and which may contain material not suitable to be viewed for audience under 18
Advertisements	Non Working	Sites providing advertising graphics or other pop ad content files
AlcoholandTobacco	Non Working	Sites providing information about, promote, or support the sale of alcoholic beverages or tobacco products or associated paraphernalia
ALLWebTraffic	Neutral	Any HTTP Traffic
Applets	Non Working	All web pages contains Applets
ArtsAndHistory	Non Working	Sites primarily exhibiting artistic techniques like creative painting, sculpture, poetry, dance, crafts, Literature, and Drama. Sites that narrate historical details about countries/places; events that changed the course of history forever; sites providing details and events of all wars i.e. World Wars, Civil Wars, and important persons of



		world historical importance
Astrology	Non Working	Sites showing predictions about Sun signs and into various subjects like Education & Career, Love Relationships, etc.
BusinessAndEconomy	Neutral	Sites sponsored by or devoted to business firms, business associations, sites providing details for all types of industrial sector like Chemicals, Machinery, Factory Automation, Cable and Wire, sites providing information about couriers and logistics, and Non-Alcoholic Soft drinks and Beverages
Chat	Non Working	Sites hosting Web Chat services or providing support or information about chat via HTTP or IRC
CommercialBanks	Neutral	Commercial Banks Category includes all Banking Sites i.e. International / National Public or Private Sector Banks providing a wide range of services such as all types of Accounts and Cards, Fixed Deposits, and Loans
Communication	Neutral	Sites offering telephone, wireless, long distance, and paging services. It also includes sites providing details about Mobile communications / cellular communications
ComputerSecurityAndHacking	Productive	Sites providing information about hacking, computer security, sites providing Anti-Virus solutions, including sites providing information about or promote illegal or questionable access to or use of computer or communication equipment, software, or databases
Cookies	Non Working	Includes all cookie based web pages
Cricket	Non Working	Sites providing Live Scores of cricket matches, Debates on Cricketers, Top 10 Cricketers, Cricket News, and forthcoming Cricket matches. Cricket Category is differentiated from Sports Category and solely devoted to Cricket activities
CrimeAndSuicide	UnHealthy	Advocating, instructing, or giving advice on performing illegal acts such as phone, service theft, evading law enforcement, lock-picking, burglary techniques and suicide
CulturalInstitutions	Neutral	Sites sponsored by museums, galleries, theatres , libraries, and similar institutions; also, sites whose purpose is the display of artworks
DatingAndMatrimonials	Non Working	Sites assisting users in establishing interpersonal relationships, friendship, excluding those of exclusively gay, or lesbian or bisexual interest and Matrimonial Sites providing photos and details of individuals seeking life partners
DownloadFreewareAndShareware	UnHealthy	Sites whose primary purpose is providing freeware and shareware downloads of application, software, tools, screensavers, wallpapers, and drivers
Drugs	UnHealthy	Sites providing information about the

		cultivation, preparation, or use of prohibited drugs
EducationalInstitutions	Productive	Sites sponsored by schools, colleges, institutes, online education and other educational facilities, by non-academic research institutions or that relate to educational events and activities
EducationAndReferenceMaterial	Productive	Sites offering books, reference-shelf content such as atlases, dictionaries, encyclopedias, formularies, white and yellow pages, and public statistical data
Electronics	Neutral	Sites providing information on manufacturing of electronics and electrical equipments, gadgets, instruments like air conditioners, Semi conductors, Television, Storage Devices, LCD Projectors, Home Appliances, and Power Systems etc.
Entertainment	Non Working	Sites providing entertainment sources for Movies, Celebrities, Theatres, about or promote motion pictures, non-news radio and television, humor, Comics, Kids and Teen amusement, Jokes, and magazines
Finance	Non Working	Sites providing information on Money matters, investment, a wide range of financial services, economics and accounting related sites and sites of National & International Insurance companies providing details for all types of Insurances & Policies
Gambling	UnHealthy	Sites providing information about or promote gambling or support online gambling, involving a risk of losing money
Games	Non Working	Sites providing information about or promote electronic games, video games, computer games, role-playing games, or online games
Government	Neutral	Sites sponsored by countries, government, branches, bureaus, or agencies of any level of government including defence. Government associated Sites providing comprehensive details on Tax related issues excluding Government sites providing Visa and Immigration services
HealthAndMedicines	Productive	Sites providing information or advice on personal health and fitness. Sites of pharmaceutical companies and sites providing information about Medicines
HobbiesAndRecreation	Non Working	Sites providing information about or promote private and largely sedentary pastimes, but not electronic, video, or online games. Homelife and family-related topics, including parenting tips, gay/lesbian/bisexual (non-pornographic sites), weddings, births, and funerals Foreign cultures, socio-cultural information
HTTPUpload	Non Working	HTTP Upload Restriction
HumanRightsandLiberty	Neutral	Sites advocating sand protecting Human Rights and Liberty to prevent discrimination

		and protect people from inhumane
ImageBanks	Non Working	Image Banks
InformationTechnology	Productive	Sites sponsoring or providing information about computers, software applications, database, operating system. Including sites providing information of hardware, peripherals, and services. Sites offering design, flash, graphics, multimedia, and web site designing tutorials, tools, advice and services
InstantMessages	Non Working	Sites enabling instant messaging
IPAddress	Neutral	
ISPWebHosting	Neutral	Sites enabling users to make telephone, lease line, ISDN, Cable, V-SAT connections via Internet or obtaining information for that purpose. Sites providing hosting services, or top-level domain pages of Web communities
JobsSearch	UnHealthy	Sites offering information about or support the seeking of employment or employees
Kids	Neutral	Sites designed specifically for kids
MilitancyAndExtremist	UnHealthy	Sites offering information about groups advocating antigovernment beliefs or action
Music	Non Working	Sites providing songs and music and supporting downloads of MP3 or other sound files or that serve as directories of such sites
NatureAndWildLife	Non Working	Sites providing information about Nature, explorations, discoveries, wild life, animals, birds, protecting endangered species, habitats, Animal sanctuaries, etc.
NewsAndMedia	Neutral	Sites offering current news and opinions, including those sponsored by newspapers, general-circulation magazines or other media. It also includes sites of advertising agencies and sites providing details of weather forecast
None	Neutral	Uncategorized Traffic
Nudity	UnHealthy	Sites depicting nude or seminude human forms, singly or in groups, not overtly sexual in intent or effect. It includes Nude images of film stars, models, nude art and photography
PersonalAndBiographySites	Non Working	Includes personal sites of individuals and biographical sites of ordinary or famous personalities
PhishingAndFraud	UnHealthy	Sites gathering personal information (such as name, address, credit card number, school, or personal schedules) that may be used for malicious intent
PhotGalleries	Non Working	Sites providing photos of celebrities, models, and well-known personalities Such sites may also contain profiles or additional elements as long as the primary focus is on multi-celebrity photographs
PoliticalOrganizations	Neutral	Sites sponsored by or providing information about political parties and interest groups focused on elections or legislation

Porn	UnHealthy	Sites depicting or graphically describing sexual acts or activity, including exhibitionism and sites offering direct links to such sites. Sites providing information or catering Gay, Lesbian, or Bisexual images and lifestyles are also included in this category
Portals	Non Working	Portals include web sites or online services providing a broad array of resources and services such as search engines, free email, shopping, news, and other features
PropertyAndRealEstate	Neutral	Sites providing information about renting, buying, selling, or financing residential, real estate, plots, etc.
Science	Productive	Sites providing news, research projects, ideas, information of topics pertaining to physics, chemistry, biology, cosmology, archeology, geography, and astronomy
SearchEngines	Neutral	Sites supporting searching the Web, groups, or indices or directories thereof
SeXHealthAndEducation	Neutral	Sites providing information regarding Sexual Education and Sexual Health and sites providing Medicines to cure and overcome Sex related problems and difficulties, with no pornographic intent
SharesAndStockMarket	Non Working	Sites providing charting, market commentary, forums, prices, and discussion of Shares and Stock Market. It also includes sites dealing in online share trading and sites of stockbrokers
Shopping	Non Working	Sites supporting Online purchases of consumer goods and services except: sexual materials, lingerie, swimwear, investments, medications, educational materials, computer software or hardware. Also Sites of Showrooms, Stores providing shopping of consumer products
Spirituality	Non Working	Sites featuring articles on healing solutions in wellness, personal growth, relationship, workplace, prayer, articles on God, Society, Religion, and ethics
Sports	Non Working	Sites providing any information about or promoting sports, active games, and recreation. All types of Sites providing information about Sports except Cricket
SpywareAndP2P	UnHealthy	Sites or pages that download software that, without the user's knowledge, generates http traffic (other than simple user identification and validation) and Sites providing client software to enable peer-to-peer file sharing and transfer
SwimwareAndLingerie	Non Working	Sites showing images of models and magazines offering lingerie/swimwear but not Nude or sexual images. It also includes Arts pertaining Adult images and shopping of lingerie
TravelFoodAndImmigration	Non Working	Sites providing information about traveling

		i.e. Airlines and Railway sites. Sites providing details about Hotels, Restaurants, Resorts, and information about worth seeing places. Sites that list, review, advertise, or promote food, dining, or catering services. Sites providing Visa, Immigration, Work Permit and Holiday & Work Visa details, procedures and services
URLTranslationSites	UnHealthy	Sites offering Online translation of URLs. These sites access the URL to be translated in a way that bypasses the proxy server, potentially allowing unauthorized access
Vehicles	Non Working	Sites providing information regarding manufacturing and shopping of vehicles and their parts
Violence	UnHealthy	Sites featuring or promoting violence or bodily harm, including self-inflicted harm; or that gratuitously displaying images of death, gore, or injury; or featuring images or descriptions that are grotesque or frightening and of no redeeming value. These do not include news, historical, or press incidents that may include the above criteria
Weapons	UnHealthy	Sites providing information about, promote, or support the sale of weapons and related items
WebBasedEmail	Non Working	Sites providing Web based E-mail services or information regarding email services

## File Types Category

File type is a grouping of file extensions. Cyberoam allows filtering Internet content based on file extension. For example, you can restrict access to particular types of files from sites within an otherwise-permitted category.

For your convenience, Cyberoam provides several default File Types categories. You can use these or even create new categories to suit your needs.

Depending on the organization requirement, allow or deny access to the categories with the help of policies by groups, individual user, time of day, and many other criteria.

- [Create Custom File Type category](#)
- [Manage Custom File Type category](#)
- [Manage Default File Type category](#)

### Create Custom File Type category

Use to:

- Create custom file type category
- Update custom file type category

#### To create custom file type category

1. Select **Categories → File Type Category → Create Custom**
2. Enter name for the file type category
3. Enter the file extensions to be included in the category.  
Multiple extensions can be entered using comma e.g. bmp,,jpeg
4. Enter relevant description
5. Click Create/Update to save the details

**Create Custom File Type Category** Register

**Create Custom File Type Category**

Name\*

File Extensions\*

Description

**Create** **Cancel**

## To update Custom File Type category

1. Select **Categories → File Type Category → Manage Custom** to view the list of custom categories and click category to be modified
2. Displays category name which cannot be modified
3. Change the extension as per the requirement
4. Change the description, if required.
5. Click Update if any modifications are done

## Manage Custom File Type category

Use to:

- Modify Description
- Add/Remove file extensions from custom category
- Assign File type category to a Device
- Delete custom category. Deleting custom file type category will delete from the Cyberoam Central Console and not from the devices.

## To assign File Type Category to a Device

1. Select **Categories → File Type Category → Manage Custom**
2. Click Apply against the File type category name. It opens a new page and displays group wise devices. Enable the check box against the group or device to which the File type category is to be added.
3. Click Apply. Applied will be displayed against the group/device, if the File type category is added successfully.

## To delete File Type Category



**Not attached to any policy**

1. Select **Categories → File Type Category → Manage Custom** to view the list of categories
2. Click Select against the category to be removed OR Click Select All to remove all the categories
3. Click Delete

Deleting custom file type category will delete from the Cyberoam Central Console and not from the devices.

## Manage Default File Type category

Cyberoam provides five default File Type categories which cannot be modified or deleted.

To view the list of default file type categories and extensions included in them, go to **Categories → File Type Category → Manage Default**

## Application Protocol Category

Application Protocol Category is the grouping of Application Protocols used for filtering Internet content.

You can also filter Internet requests based on protocols or applications other than HTTP, HTTPS or FTP, for example those used for instant messaging, file sharing, file transfer, mail, and various other network operations.

For your convenience, Cyberoam provides a database of default Application Protocol categories. To use the default Application Protocol categories, the add-on module 'Web and Application Filter' should be registered.

- [Create Custom Application Protocol category](#)
- [Manage Custom Application Protocol category](#)
- [Manage Default Application Protocol category](#)

### Create Custom Application Protocol category

Use to

- Create custom application protocol category
- Update custom application protocol category

#### To create custom application protocol category

1. Select **Categories** → **Application Protocol Category** → **Create Custom**
2. Enter category name



**Custom category name and Default category name cannot be same**

3. Enter relevant description
4. Click Create to save the details
5. Click Add to enter the application protocol details. (See To add Application Protocol category details)

Create Custom Application Protocol Category		Logout	Help
Create Custom Application Protocol Category			
Name*	<input type="text"/>		
Description	<input type="text"/>		
Create		Cancel	



**Edit Custom Protocol Category** Logout Help Cyberoam

**Update Custom Application Category**

Name\* MyCategory

Description

**Application Detail**

Application	Destination IP

Add

Update Cancel

### To update Custom of Application protocol category

1. Select **Categories → Application Protocol Category → Manage Custom** to view the list of custom categories and click category to be modified
2. Displays category name which cannot be modified
3. Change the description, if required.
4. Under Custom Application protocol details  
Click Add to add protocol details. (See To add Application Protocol category details)  
To delete details see To delete application protocol details.
5. Click Update if any modifications are done

**Manage Custom Application Protocol Category** CCC Help Logout

Category Name	Description
Spark	

Delete Apply Del

**Edit Custom Protocol Category** CCC Help Logout

**Update Custom Application Protocol Category**

Name\* Spark

Description

**Custom Application Protocol Details**

Application	Destination IP
jabber	203.188.195.30

Add Del

Delete

Update Cancel

### To add Application Protocol category details

1. Click Add if adding details at the time of creation of the Category OR Select **Policy Settings → Application protocol → Manage Custom** and click protocol name to which details is to be added, if adding details after the creation of protocol
2. Select Application  
Both Custom and Standard application protocol can be grouped in a single Application Protocol Category  
To create custom application protocol, see Define Custom Application Protocol
3. Enter destination IP/Network address for the protocol.
4. Click Add to save

**Custom Application Protocol Details**

Application\* Select Application

Destination IP/Network Address\* ( \* for all)

**Add** **Cancel**

## Manage Custom Application Protocol category

Use to:

- Modify Description
- Add details to Application protocol category
- Assign to a Device
- Delete details to Application protocol category
- Delete custom category. Deleting custom application protocol category will delete from the Cyberoam Central Console and not from the devices.

### To assign Application protocol category to a Device

1. Select **Categories** → **Application Protocol Category** → **Manage Custom**
2. Click Apply against the Application protocol category name. It opens a new page and displays group wise devices. Enable the check box against the group or device to which the Application protocol category is to be added.
3. Click Apply. Applied will be displayed against the group/device, if the Application protocol category is added successfully.

**Manage Custom Application Protocol Category**

Category Name	Description	Apply	Del
Spark		<b>Apply</b>	<b>Delete</b>

**Select Device**

- ☐ General
  - ☐ StandbyUnit
- ☐ USBBranches
  - ☐ USBBranch1
  - ☐ USBBranch2
- ☐ INBranches
  - ☐ BlrBranch1
  - ☐ DelhiBranch1
- ☐ HeadOffices
  - ☐ USHeadOffice
  - ☐ INHeadOffice

**Apply** **Close**

## To delete Application Protocol Category



**Not attached to any policy**

1. Select **Categories** → **Application Protocol Category** → **Manage Custom** to view the list of custom categories
2. Click Select against the category to be removed OR Click Select All to remove all the categories
3. Click Delete



**Only customized Application protocol category can be modified or deleted**

Deleting custom application protocol category will delete from the Cyberoam Central Console and not from the devices.

Manage Custom Application Protocol Category		ccc	Help	Logout
Category Name	Description	Apply	Del	
Spark		Apply	<input checked="" type="checkbox"/>	Delete

## To delete application protocol details

1. Select **Categories** → **Application Protocol Category** → **Manage Custom** to view the list of categories and click Category from which the details is to be removed
2. Click Select against the details(s) to be removed OR Click Select All to remove all
3. Click Delete

Application Detail			Add
Application	Destination IP	Del	
ftp	ALL	<input type="checkbox"/>	
http	ALL	<input type="checkbox"/>	
		Select All	<input type="checkbox"/>
			Delete

## Manage Default Application protocol category

Default Application protocol categories are available for use only if 'Web and Application Filter' add-on module is registered. Check Licensing for details. Database of protocol category is constantly updated by Cyberoam.

Default Application protocol category cannot be modified or deleted.

To view the list of default Application protocols, go to Categories → Application protocol category → Manage Default

# Policies

Cyberoam allows controlling access to various resources with the help of Policy. These policies can be created and applied to Cyberoam from Cyberoam Central Control.

Types of policies:

1. Control web access by defining Internet Access policy. (See [Internet Access policy](#) for more details)
2. Allocate and restrict the bandwidth usage by defining Bandwidth policy. (See [Bandwidth policy](#) for more details)

Cyberoam comes with several predefined policies. These predefined policies are immediately available for use until configured otherwise.

Cyberoam also lets you define following customized policies to define different levels of access for different users to meet your organization's requirements:

- [Internet Access policy](#)
- [Bandwidth policy](#)

## Schedule

Schedule defines a time schedule for applying firewall rule or Internet Access policy i.e. used to control when firewall rules or Internet Access policies are active or inactive.

Types of Schedules:

- Recurring – use to create policies that are effective only at specified times of the day or on specified days of the week.
  - One-time - use to create firewall rules/policies that are effective once for the period of time specified in the schedule.
- 
- [Define Schedule](#)
  - [Manage Schedule](#)

### Define Schedule

Use to:

- [Create Schedule](#)
- Update Schedule

### To create schedule

1. Select **Policies → Schedule → Create**
2. Enter Schedule name that best describes the schedule
3. Select Schedule Type
  - Recurring – use to create policies that are effective only at specified times of the day or on specified days of the week.

- One-time - use to create firewall rules/policies that are effective once for the period of time specified in the schedule
4. Enter relevant description for the schedule
  5. Click Create
  6. On successful creation, Click Add to add a new schedule entry details. (See [To add a Schedule Entry detail](#))

### Define Schedule

Schedule Details

Name*	<input style="width: 90%;" type="text"/>
Schedule Type*	<input type="radio"/> Recurring <input checked="" type="radio"/> One Time
Start Time	<div style="display: flex; align-items: center;"> <div style="border: 1px solid #ccc; padding: 2px 5px; margin-right: 5px;">May 16, 2007</div> <div style="border: 1px solid #ccc; padding: 2px 5px; margin-right: 5px;">00</div> <div style="border: 1px solid #ccc; padding: 2px 5px; margin-right: 5px;">00</div> <div style="margin-left: 5px;">  Calendar         </div> </div>
Stop Time	<div style="display: flex; align-items: center;"> <div style="border: 1px solid #ccc; padding: 2px 5px; margin-right: 5px;">May 16, 2007</div> <div style="border: 1px solid #ccc; padding: 2px 5px; margin-right: 5px;">00</div> <div style="border: 1px solid #ccc; padding: 2px 5px; margin-right: 5px;">00</div> <div style="margin-left: 5px;">  Calendar         </div> </div>
Description	<div style="border: 1px solid #ccc; height: 60px; width: 95%;"></div>

Create

### To add Schedule Entry details

1. Click Add if adding details at the time of creation of the Schedule OR
2. Select **Policies → Schedule → Manage** and click schedule name to which details is to be added, if adding details after the creation of Schedule
3. Select the schedule occurrence i.e. on which weekdays and at what time schedule will be applicable
 

In Weekdays, select any one option

  - Weekdays – Schedule will be applied from Monday to Friday
  - Weekdays including Saturday – Schedule will be applied from Monday to Saturday
  - All Days of Week – Schedule will be applied from Monday to Sunday
  - Selected Weekday(s) - Schedule will be applied on selected days only
4. Enter Start and Stop time. Stop time cannot be greater than start time
5. Click Add Schedule Details to save the details

## Manage Schedule

Use to:

- Update Schedule name and description
- Assign Schedule to Device
- Delete Schedule. Deleting schedule will delete schedule from the Cyberoam Central Console and not from the devices.
- Add Schedule Entry details
- Delete Schedule Entry details

### To update Schedule

1. Select **Policies** → **Schedule** → **Manage** and click Schedule name to be updated
2. Change the schedule name, if required.
3. Change the schedule description, if required.
4. Click Add to add a new schedule entry details. (See To add a Schedule Entry detail)
5. Click Delete to delete the selected schedule entry details. (See To delete a Schedule Entry detail)
6. Click Save if any modifications are done.

Manage Schedule
CCC
Help
Logout

Schedule Name	Schedule Type	Description	Apply	Del
All the time	Recurring	All the time	-	-
Work hours (5 Day week)	Recurring	5 days working week 10:00 to 19:00.	Apply	<input type="checkbox"/>
Work hours (6 Day week)	Recurring	6 days working week 10:00 - 19:00 i.e. Monday to Saturday	Apply	<input type="checkbox"/>

Edit Schedule
CCC
Help
Logout

Schedule Details

Name\*
Work hours (5 Day week)

Schedule Type\*
Recurring

Description
5 days working week 10:00 to 19:00.

Schedule Entry

Add

Weekday	Start time(HH:mm)	Stop time(HH:mm)	Del
Week Days	10:00	19:00	<input type="checkbox"/>

Delete

Save

Cancel

## To assign Schedule to a Device

1. Select **Policies → Schedule → Manage**
2. Click Apply against the Schedule name. It opens a new page and displays group wise devices. Enable the check box against the group or device to which the Schedule is to be added.
3. Click Apply. Applied will be displayed against the group/device, if the Schedule is added successfully.

The screenshot shows the 'Manage Schedule' page with the following table:

Schedule Name	Schedule Type	Description	Apply	Del
All the time	Recurring	All the time	-	-
Work hours (5 Day week)	Recurring	5 days working week 10:00 to 19:00.	Apply	
Work hours (6 Day week)		10:00 i.e. Monday	Apply	

The 'Select Device' modal window displays the following structure:

- ☐ General
  - ☐ StandbyUnit (XXXXXXXXXX)
- ☐ USBranches
  - ☐ USBranch1 (XXXXXXXXXX)
  - ☐ USBranch2 (XXXXXXXXXX)
- ☐ INBranches
  - ☐ BlrBranch1 (XXXXXXXXXX)
  - ☐ DelhiBranch1 (XXXXXXXXXX)
- ☐ HeadOffices
  - ☐ USHeadOffice (XXXXXXXXXX)
  - ☐ INHeadOffice (XXXXXXXXXX)

Buttons: Apply, Close, Delete

## To delete Schedule Entry details

1. Select **Policies** → **Schedule** → **Manage** and click schedule name from which details is to be removed
2. Click Select against the entry detail(s) to be deleted OR Click Select All to delete all entry details
3. Click Delete

**Edit Schedule** CCC Help Logout

**Schedule Details**

Name\* Work hours (5 Day week)

Schedule Type\* Recurring

Description 5 days working week 10:00 to 19:00.

**Schedule Entry**

Weekday	Start time(HH:mm)	Stop time(HH:mm)	Del
Week Days	10:00	19:00	<input checked="" type="checkbox"/>

Add Delete Save Cancel

## To delete Schedule



### Not assigned to any policy

1. Select **Policies** → **Schedule** → **Manage** to view the list of Schedules
2. Click Select against the schedule(s) to be deleted OR Click Select All to delete all the schedules
3. Click Delete



### Default policy cannot be updated or deleted

Deleting schedule will delete schedule from the Cyberoam Central Console and not from the devices.

**Manage Schedule** CCC Help Logout

Schedule Name	Schedule Type	Description	Apply	Del
All the time	Recurring	All the time	-	-
Work hours (5 Day week)	Recurring	5 days working week 10:00 to 19:00.	Apply	<input checked="" type="checkbox"/>
Work hours (6 Day week)	Recurring	6 days working week 10:00 - 19:00 i.e. Monday to Saturday	Apply	<input type="checkbox"/>
Select All				<input type="checkbox"/>

Delete



## Internet Access Policy

Internet Access policy controls user's web access. It specifies which user has access to which sites or applications and allows defining powerful security policies based on almost limitless policy parameters like:

- Individual users
- Groups of users
- Time of day
- Location/Port/Protocol type
- Content type
- Bandwidth usage (for audio, video and streaming content)

Allow/deny access to an entire application category, or individual file extensions within a category with the help of policy. For example, you can define a policy that blocks access to all audio files with .mp3 extensions.

Two strategies based on which Internet Access policy can be defined:

**Allow 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 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.

- [Create Internet Access policy](#)
- [Manage Internet Access policy](#)
- [Default Internet policy](#)

### Create Policy

Use to:

- Create Internet Access policy
- Update Internet Access policy

### To create Internet Access policy

1. Select **Policies → Internet Access Policy → Create Policy**
2. Enter policy name



**Policies with the same name cannot be created**

3. Select Template based on which you want to create new policy  
Select a template if you want to create a new policy based on an existing policy and want to inherit all the categories restrictions from the existing policy

Select 'Blank' template, if you want to create a fresh policy without any restrictions. After creation you can always customize the category restrictions according to the requirement.

4. Specify strategy to be applied for the policy.  
Allow – Allows access to all the categories except the specified categories.

**This option is available only if you are creating policy using 'Blank' template**

- In Category Name column,  
**W** represents Web Category  
**F** represents File Type Category  
**A** represents Application Protocol Category  
**D** represents Default Category  
**C** represents Customized i.e. User defined

CCC

Help

Logout

## Edit Internet Access Policy

Internet Access Policy 'Sample policy' has been created successfully

Internet Access Policy Details

Name\*

Sample policy

Policy Type\*

Allow

Description

Reporting

☒ Enable
 ☐ Disable

Internet Access Policy Rules

Category Name	Strategy	During Schedule	
			<div>Add</div> <div>Del</div>

Save

Cancel

## To update Internet Access policy

1. Select **Policies → Internet Access Policy → Manage Policy** to view the list of policies and click policy to be modified
2. Displays policy name which cannot be modified
3. Displays policy type which cannot be modified
4. Change the description, if required.
5. Under Internet Access Policy Rules  
Click Add to add protocol details. (See To add policy rules)  
To delete policy rule, see To delete policy rule  
To change rule order, see To change the order

In Category Name column,

**W** represents Web Category

**F** represents File Type Category

**A** represents Application Protocol Category

**D** represents Default Category

**C** represents Customized i.e. User defined Category

6. Click Save if any modifications are done
7. Click Show Policy Members to view the list of users to whom the policy is assigned



**The changes made in the policy become effective immediately on saving the changes**

**Manage Internet Access Policy** CCC Help Logout

Internet Access Policy Name	Default Strategy	Description	Apply	Reporting	Del
<u>Accounting &amp; Finance Department</u>	Deny	to allow accounting / financial / my company websites.	Apply	Enabled	<input type="checkbox"/>
<u>Admin , Legal &amp; Account Group policy</u>	Deny	This is applicable for Admin, Legal and Account Departments jointly.	Apply	Enabled	<input type="checkbox"/>
<u>Administrators policy</u>	Allow	Applicable to all system, network and data center administrators.	Apply	Enabled	<input type="checkbox"/>

**Edit Internet Access Policy** CCC Help Logout

**Internet Access Policy Details**

Name\* Accounting & Finance Department

Policy Type\* Deny

Description  
to allow accounting / financial / my company websites.

Reporting ☒ Enable ☐ Disable

**Internet Access Policy Rules**

**Rule Details**

Select Category\* Web Category: Porn, Advertisements, SexHealthAndEducation, PersonalAndBiographySites, Music, WebBasedEmail

File Type Category: Video Files, Audio Files, Executable Files, Dynamic Files, Image Files, MP3Files

Application Protocol Category: Yahoo Messenger, AOL Messenger, MSN Messenger, All Chat Applications, P2P Applications, Streaming Media

Strategy: Select Strategy

During Schedule: Select Schedule

[View Details](#)

**Add Cancel**

## To add Policy rule

1. Click Add if adding rules at the time of creation of the policy OR  
Select **Policies** → **Internet Access Policy** → **Manage Policy** and click policy name to which rule is to be added, if adding after the creation of policy
2. Under the Category option  
Select Web Category to be assigned to the policy. Use Ctrl/Shift and click to select the multiple categories.



**If 'Web and Application Filter' add-on module is registered, all the default Categories will also be listed and can be used for restriction**

Select File Type Category to be assigned to the policy. Use Ctrl/Shift and click to select the multiple categories.

Select Application Protocol Category to be assigned to the policy. Use Ctrl/Shift and click to select the multiple categories.



**If 'Web and Application Filter' add-on module is registered, all the default Categories will also be listed and can be used for restriction**

3. Specify rule strategy to be applied during the scheduled time interval.  
Allow – Allows the Internet access during the scheduled time interval  
Deny – Does not allow the Internet access during the scheduled time interval
4. Select Schedule  
Depending on the rule strategy, access to the selected categories will be allowed/denied for the scheduled time interval. If you are not sure about the schedule details, select schedule and click View details link to view the schedule details.
5. Click Add to create and save the rule

## Manage Policy

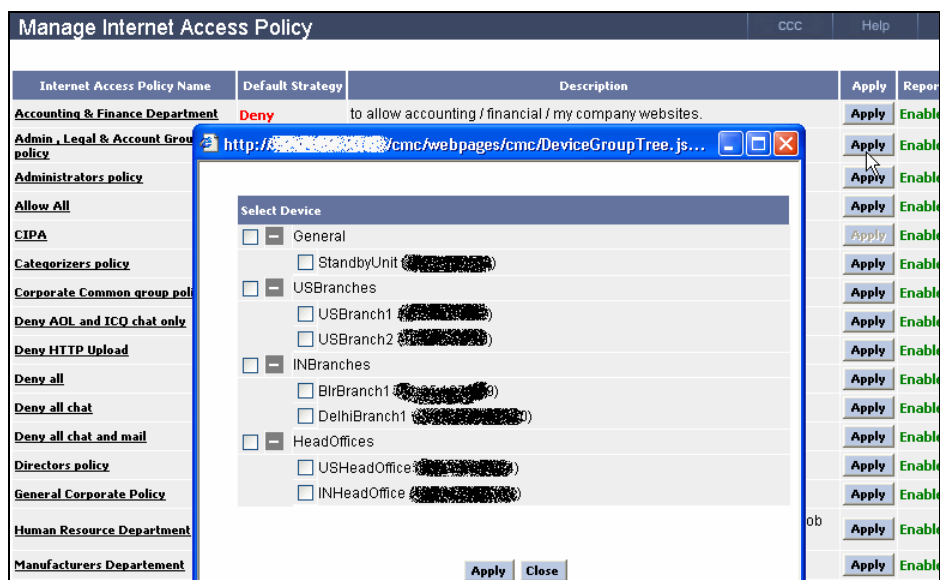
Manage policy page displays list of predefined as well as customized policies created. Predefined policies can also be modified as per the requirement.

Use Internet Access Policy > Manage Policy to:

- Assign Internet Access policy to a Device
- Delete policy rule
- Delete Policy. Deleting policy will delete from the Cyberoam Central Console and not from the devices.

### To assign Internet Access policy to a Device

1. Select **Policies** → **Internet Access policy** → **Manage**
2. Click Apply against the Internet Access policy name. It open as a new page and displays group wise devices. Enable the check box against the group or device to which the Internet Access policy is to be added.
3. Click Apply. Applied will be displayed against the group/device, if the Internet Access policy is added successfully.



### To delete Internet Access policy rule

1. Select **Policies** → **Internet Access Policy** → **Manage policy** to view the list of policies and click the policy from which the rule is to be deleted
2. Click Del against the rule to be deleted OR Click Select All to delete all the rules
3. Click Delete

Internet Access Policy Rules				
				<input type="button" value="Add"/> <input type="button" value="Delete"/>
Category Name	Strategy	Description	During Schedule	Del
Porn (W/D)	Deny	Porn Sites	All the time	<input type="checkbox"/>
Games (W/D)	Deny	Games	All the time	<input type="checkbox"/>
Advertisements (W/D)	Deny	Advertisement	All the time	<input checked="" type="checkbox"/>
				<input type="button" value="MoveUp"/> <input type="button" value="MoveDown"/> <input type="button" value="Update"/>
				<input type="button" value="Select All"/>

### To delete Internet Access policy



#### Not assigned to any Group

1. Select **Policies** → **Internet Access Policy** → **Manage policy** to view the list of policies
2. Click Del against the policy to be deleted OR Click Select All to delete all the policies
3. Click Delete

Deleting policy will delete from the Cyberoam Central Console and not from the devices.

Manage Internet Access Policy					ccc	Help	Logout
Internet Access Policy Name	Default Strategy	Description	Apply	Reporting	Del		
<u>Accounting &amp; Finance Department</u>	Deny	to allow accounting / financial / my company websites.	<input type="button" value="Apply"/>	Enabled	<input checked="" type="checkbox"/>		
<u>Admin , Legal &amp; Account Group policy</u>	Deny	This is applicable for Admin, Legal and Account Departments jointly.	<input type="button" value="Apply"/>	Enabled	<input checked="" type="checkbox"/>		
<u>Administrators policy</u>	Allow	Applicable to all system, network and data center administrators.	<input type="button" value="Apply"/>	Enabled	<input type="checkbox"/>		
<u>Allow All</u>	Allow	Allow all Internet Access	<input type="button" value="Apply"/>	Enabled	-		
<u>CIPA</u>	Allow	Internet Access Policy for Children's Internet Protection Act	<input type="button" value="Apply"/>	Enabled	-		
<u>Categorizers policy</u>	Allow	Applicable for Categorizers Department	<input type="button" value="Apply"/>	Enabled	<input type="checkbox"/>		
<u>Corporate Common group policy</u>	Allow	Default policy applies to default group.	<input type="button" value="Apply"/>	Enabled	<input type="checkbox"/>		
<u>Deny AOL and ICQ chat only</u>	Allow	Deny AOL and ICQ Chat Only	<input type="button" value="Apply"/>	Enabled	<input type="checkbox"/>		
<u>ccciap</u>	Allow		<input type="button" value="Apply"/>	Enabled	<input type="checkbox"/>		
					<input type="button" value="Select All"/>		
					<input type="button" value="Delete"/>		

## Bandwidth Policy

Bandwidth is the amount of data passing through a media over a period of time and is measured in terms of kilobytes per second (kbps) or kilobits per second (kbits) (1 Byte = 8 bits).

The primary objective of bandwidth policy is to manage and distribute total bandwidth on certain parameters and user attributes. Bandwidth policy allocates & limits the maximum bandwidth usage of the user and controls web and network traffic.

To configure Bandwidth policy:

- [Define for whom you want to create policy](#)
- [Define Type of policy](#)
- [Define the Implementation strategy of the policy](#)
- [Define Bandwidth Usage](#)

### Policy can be defined/created for:

- Logon Pool - It restricts the bandwidth of a Logon Pool i.e. all the users defined under the Logon Pool share the allocated bandwidth.
- User - It restricts the bandwidth of a particular user.
- Firewall Rule - It restricts the bandwidth of any entity to which the firewall rule is applied.

### Types of Policy

(Only for when policy is based on/created for User or IP address)

Two types of bandwidth restriction can be placed:

1. Strict  
In this type of bandwidth restriction, user cannot exceed the defined bandwidth limit.
2. Committed  
In this type of bandwidth restriction, user is allocated the guaranteed amount of bandwidth and can draw bandwidth up to the defined burstable 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 burstable rate. Guaranteed rates also assure minimum bandwidth to critical users to receive constant levels of bandwidth during peak and non-peak traffic periods.

Guaranteed represents the minimum guaranteed bandwidth and burstable represents the maximum bandwidth that the user can use, if available.

### Implementation strategy

(Only for when policy is based on/created for User or IP address)

Policy can be implemented in two ways depending on policy Type:

- Total (Upstream + Downstream)
- Individual Upstream and Individual Downstream

**Strict policy**

Implementation on	Bandwidth specified	Example
Total (Upstream + Downstream)	Total bandwidth	Total bandwidth is 20 kbps upstream and downstream combined cannot cross 20 kbps
Individual Upstream and Individual Downstream	Individual bandwidth i.e. separate for both	Upstream and Downstream bandwidth is 20 kbps then either cannot cross 20 kbps

**Committed policy**

Implementation on	Bandwidth specified	Example
Total (Upstream + Downstream)	Guaranteed bandwidth	Guaranteed bandwidth is 20 kbps upstream and downstream combined will get 20 kbps guaranteed (minimum) bandwidth
	Burstable bandwidth	Burstable bandwidth is 50 kbps upstream and downstream combined can get up to 50 kbps of bandwidth (maximum), if available
Individual Upstream and Individual Downstream	Individual Guaranteed and Burstable bandwidth i.e. separate for both	Individual guaranteed bandwidth is 20 kbps Individually get 20 kbps guaranteed (minimum) bandwidth  Individual burstable bandwidth is 50 kbps Individually get maximum bandwidth up to 50 kbps, if available

**Bandwidth Usage**

(Only for when policy is based on/created for User or IP address)

Policy can be configured for two types of bandwidth usage:

Individual – Allocated bandwidth is for the particular user only

Shared – Allocated bandwidth is shared among all the users who have been assigned this policy

- [Create Bandwidth policy](#)
- [Manage Bandwidth policy](#)

**Create Policy**

Use to:

- Create Bandwidth policy
- Update Bandwidth policy



## To create Bandwidth policy

1. Select **Policies → Bandwidth Policy → Create Policy**
2. Enter policy name



**Policies with the same name cannot be created**

3. Select any one option to specify for whom the policy is to be created.
  - Logon Pool based policy restricts the bandwidth of a Logon Pool i.e. all the users defined under the Logon Pool share the allocated bandwidth.
  - User based policy restricts the bandwidth of a particular user.
  - IP address based restricts the bandwidth for a particular IP address.

4. Select any one option to specify policy type

Strict

In this type of policy, user cannot exceed the defined bandwidth limit.

Committed

In this type of policy, user is allocated the guaranteed amount of bandwidth and can draw bandwidth up to the defined burstable 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 burstable rate. Guaranteed rates also assure minimum bandwidth to critical users to receive constant levels of bandwidth during peak and non-peak traffic periods.

Guaranteed represents the minimum guaranteed bandwidth and burstable represents the maximum bandwidth that the user can use, if available.



**This option is available only for User or IP address based policy**

5. Select any one option to specify implementation strategy of policy. See Implementation strategy for more details



**This option is available only for User or IP address based policy**

6. Enter allowed Total or Individual and Guaranteed/Burstable bandwidth depending on Policy Type and Implementation strategy. See Implementation strategy for more details.



**This option is available only for User or IP address based policy**

7. Set the bandwidth priority
  - Priority can be set from 0 (highest) to 7 (lowest)
  - Set the priority for SSH/Voice/Telnet traffic to be highest as this traffic is more of the interaction
8. Select any one to specify the bandwidth usage
  - Individual – Allocated bandwidth is for the particular user only
  - Shared – Allocated bandwidth is shared among all the users who have been assigned this policy



**This option is available only for User or IP address based policy**

9. Enter policy description.

10. Click Create/Update to save the policy
11. Click Add Details to add schedule details to the policy. (See To add schedule details)

### To update Bandwidth policy

1. Select **Policies → Bandwidth Policy → Manage Policy** to view the list of policies and click the policy to be modified
2. Displays policy name, modify if required
3. Displays whether policy is created for Host group, user or IP address
4. Change the description, if required.
5. Displays Implementation strategy
6. Displays allocated Total or Individual and Guaranteed/Burstable bandwidth depending on Policy Type and Implementation strategy. Modify if required
7. Displays Policy Type
8. Set the bandwidth priority  
Priority can be set from 0 (highest) to 7 (lowest)  
Set priority for SSH/Voice/Telnet traffic to be highest as this traffic is more of the interaction
9. Click Update if any modifications are done
10. Click Add Details to add schedule details to the policy. (See To add schedule details)  
To remove details, see To remove schedule details



**The changes made in the policy become effective immediately on saving the changes**

Edit Bandwidth Policy		CCC	Help	Logout	
<b>Bandwidth Policy Details</b>					
Name*	128kbps link_Policy A				
Policy Based On	User Based Individual Policy				
Description	<input type="text"/>				
<b>Default Values to be applied all the time.</b>					
Implementation On	Total (Upload + download)				
Guaranteed Bandwidth (in KB)*	<input type="text" value="8"/> (between 2-4096 KB)				
Burstable Bandwidth (in KB) *	<input type="text" value="16"/> (between 2-4096 KB)				
Policy Type	Committed				
Priority*	<input type="text" value="3"/>				
<input type="button" value="Update"/> <input type="button" value="Cancel"/>					
• Add Schedule wise details to override default Bandwidth details					
Schedule	Policy Type	Bandwidth(Min/Max)	Upload Bandwidth(Min/Max)	Download Bandwidth(Min/Max)	Select
					<input type="button" value="Add Detail"/>

### To add schedule details (Only for User and IP address based Bandwidth policy)

1. Click Add Details if adding schedule at the time of creation of the policy OR  
Select **Policies** → **Bandwidth Policy** → **Manage Policy** and click policy name to which schedule is to be added, if adding after the creation of policy
2. Displays policy name
3. Displays default Policy Type set at the time of creation of policy, modify if required



**If you modify Policy Type, new policy type will override the default policy type and will be applicable only for the selected scheduled time interval.**

4. Displays default Implementation strategy set at the time of creation of policy, modify if required



**If you modify Implementation strategy, the new strategy will override the default strategy and will be applicable only for the selected scheduled time interval.**

5. Displays allocated Total or Individual and Guaranteed/Burstable bandwidth depending on Policy Type and Implementation strategy. Modify if required



**The modified bandwidth restriction will be applicable only for the selected scheduled time interval.**

6. Select Schedule during which the default policy.  
If you are not sure about the schedule details, select schedule and click View details link to view the schedule details.
7. Click Create to save the details

## Manage Policy

Manage policy page displays list of predefined as well as customized policies created. Predefined policies can also be modified as per the requirement.

Use Bandwidth Policy > Manage Policy to:

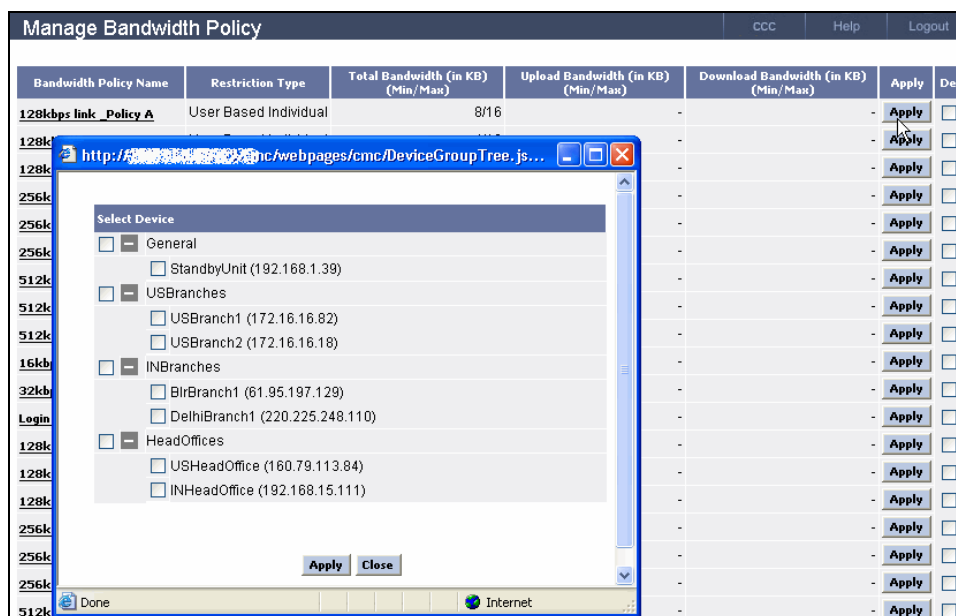
- [Add Schedule to User and IP address based policy](#)
- Assign Bandwidth policy to a Device
- Remove Schedule to User and IP address based policy
- Update allocated bandwidth
- Delete policy. Deleting policy will delete from the Cyberoam Central Console and not from the devices.

### To remove schedule details (Only for User and IP address based Bandwidth policy)

1. Select **Policies → Bandwidth Policy → Manage policy** to view the list of policies and click the policy from which the schedule is to be removed
2. Click Select against the schedule details to be removed OR Click Select All to remove all the details
3. Click Remove Details

### To assign Bandwidth policy to a Device

1. Select **Policies → Bandwidth policy → Manage policy**
2. Click Apply against the Bandwidth policy name. It opens a new page and displays group wise devices. Enable the check box against the group or device to which the Bandwidth policy is to be added.
3. Click Apply. Applied will be displayed against the group/device, if the Bandwidth policy is added successfully.



## To delete Bandwidth policy



### Not assigned to any Group/User

1. Select **Policies** → **Bandwidth Policy** → **Manage policy** to view the list of policies
2. Click Del against the policy to be deleted OR Click Select All to delete all the policies
3. Click Delete

Deleting policy will delete from the Cyberoam Central Console and not from the devices.

Manage Bandwidth Policy						CCC	Help	Logout
Bandwidth Policy Name	Restriction Type	Total Bandwidth (in KB) (Min/Max)	Upload Bandwidth (in KB) (Min/Max)	Download Bandwidth (in KB) (Min/Max)	Apply	Del		
<u>128kbps link_Policy A</u>	User Based Individual	8/16	-	-	<a href="#">Apply</a>	<input type="checkbox"/>		
<u>128kbps link_Policy B</u>	User Based Individual	4/16	-	-	<a href="#">Apply</a>	<input type="checkbox"/>		
<u>128kbps link_Policy C</u>	User Based Individual	2/16	-	-	<a href="#">Apply</a>	<input type="checkbox"/>		
<u>256kbps link_Policy A</u>	User Based Individual	16/32	-	-	<a href="#">Apply</a>	<input type="checkbox"/>		
<u>256kbps link_Policy B</u>	User Based Individual	8/32	-	-	<a href="#">Apply</a>	<input type="checkbox"/>		
<u>256kbps link_Policy C</u>	User Based Individual	2/32	-	-	<a href="#">Apply</a>	<input type="checkbox"/>		
<u>64kbps_Restricted FW</u>	Firewall Rule Based	2/8	-	-	<a href="#">Apply</a>	<input type="checkbox"/>		
<u>newhobw</u>	Firewall Rule Based	2/1024	-	-	<a href="#">Apply</a>	<input type="checkbox"/>		
						Select All	<input type="checkbox"/>	
						<a href="#">Delete</a>		

# IDP

Cyberoam is a real time Intrusion Detection and Prevention (IDP) system that protects your network from known and unknown attacks by worms and viruses, hackers and other internet risks.

Cyberoam appliance at the perimeter of your network analyzes all 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.

Cyberoam IDP consists of a signature engine with a predefined database of signatures and uses signatures to identify the malicious activity on the network. The signatures included with the Cyberoam cannot be modified.

As per your network requirements, Cyberoam allows you to define multiple policies instead of one global policy, to decrease packet latency and reduce false positives.

IDP policy allows you to view Cyberoam 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.

Cyberoam instead of providing only one policy (global) for managing multiple networks/hosts, allows to tailor the policy per network/host i.e. allows to define multiple policies for managing multiple networks/hosts. Defining multiple policies instead of one global policy helps in decreasing packet latency and reducing false positives.

To enable the intrusion detection and prevention functionality, apply the policy using firewall rule. You can create rule to apply:

- single policy for all the user/networks
- different policies for different users/networks or hosts

As firewall rules control all traffic passing through the Cyberoam and decide whether to allow or drop the connection, IDP rule will be applied to only that traffic/packet which firewall passes.

- [IDP Policy](#)

## Policy

IDP consists of a signature engine with a predefined set of signatures. Signatures are the patterns that are known to be harmful. IDP compares traffic to these signatures and responds at a high rate of speed if it finds a match. Signatures included with the Cyberoam are not modifiable.

### Category

IDP organizes signatures in categories such as DNS, Finger, P2P, DDOS, and others. These signature categories are listed in the policies. You configure these categories to change the prevention and/or detection settings. To perform Intrusion prevention and detection you need to enable IDP services for each category i.e. you will be able to configure for attack threats of individual signature only if an IDP service for the category is 'Enabled'.

Each IDP policy contains a set of signatures that the Cyberoam searches for, and log and block and allows to:

- Enable or disable category from IDP protection
- Enable or disable individual signature in a category to tailor IDP protection based on your network environment
- Define the action to be taken when the matching traffic pattern is found. Cyberoam can either detect or drop the connection. In either of the case, Cyberoam generates the log and alerts the Network Administrator.

IDP provides two modes for managing attack threats: (action if signature matches)

Drop mode - If IDP is enabled in Drop mode, Cyberoam-IDP automatically drops and resets the connection and prevents the traffic to reach its destination, if detects any traffic that matches the signature.

Detect mode - If IDP is enabled in Detect mode for a signature, Cyberoam-IDP detects and logs any traffic that matches the signature, but does not take any action against the traffic and the connection proceeds to its intended destination.

- [Create IDP Policy](#)
- [Manage IDP Policy](#)

## Create IDP Policy

Use to:

- Create IDP policy
- Enable/disable Category
- Configure individual signature
- Update IDP policy

### To create IDP policy

Create and deploy IDP policies to block malicious or suspicious traffic and increase security and productivity.

Policy allows you to view IDP signatures and configure the handling of signatures by category or on a signature-by-signature basis.

1. Select **IDP → Policy → Create**
2. Enter IDP policy name that best describes the policy
3. Enter relevant description for the policy
4. Click Create. On successful creation of policy, define what action is to be taken when the traffic matches any of the signatures.

Once you create a policy, all the signature categories are enabled but individual signatures within the category are set to 'Detect' or 'Drop' mode. You can enable/disable Category or configure individual signature for intrusion prevention and detection as and when needed.

### Create IDP Policy

IDP Policy

Name\*

lantowan\_2

Description

Create

Cancel

### Edit IDP Policy

ccc Help Logout

IDP Policy has been created successfully.

Edit IDP Policy

Name\*

lantowan\_2

Description

Category Name	Action	Enable	Edit
+ dns	-	✓	
+ finger	-	✓	
+ ftp	-	✓	
+ telnet	-	✓	
+ information	-	✓	
+ icmp	-	✓	
+ imap	-	✓	
+ dbms	-	✓	
+ sql rules	-	✓	
+ netbios	-	✓	
+ nntp	-	✓	
+ backdoor	-	✓	
+ pop	-	✓	
+ web access	-	✓	
+ smtp	-	✓	

Save

Cancel

## To Enable/Disable Category

1. Select **IDP → Policy → Manage** and click the policy for which you want to enable/disable category
2. Click Edit mark against the Category to enabled/disabled.  
 Green check mark indicates that the Category is enabled  
 Red Cross indicates that the category is disabled
3. Displays Category name and Policy name
4. In Enabled field  
 Select 'ON' to include the category for detection and/or prevention. If the Category is enabled for detection and/or prevention, Cyberoam provides maximum granularity by allowing you to change the prevention and detection settings of individual signature in the category.

Select 'OFF' to exclude the category from detection and/or prevention. Excluding the category is same as not implementing IDP for the particular category.





To enable/disable detection and/or prevention for the individual signatures, refer [To configure individual Signature](#)

- Click Save to save the configuration

**Edit IDP Policy**

Name\* lantowan\_strict

Description A Strict IDP policy for LAN to WAN Traffic

Category Name	Action	Enable	Edit
+ dns	-	✓	
+ finger	-	✓	
+ ftp	-	✓	
+ telnet	-	✓	
+ information	-	✓	
+ icmp	-	✓	
+ imap	-	✓	
+ dbms	-	✓	
+ sql rules	-	✓	
+ netbios	-	✓	
+ nntp	-	✓	
+ backdoor	-	✓	
+ pop	-	✓	
+ web access	-	✓	
+ smtp	-	✓	

**Edit IDP Category**

Category ftp

Policy lantowan\_strict

Enabled\* ON

Save Cancel

Done Internet

Save Cancel

## To configure individual Signature



### Category 'ON' for the respective Signature

- Select **IDP → Policy → Manage** to view the list of policies created. Click the policy for which you want to configure signature
- Click **+** next to the Category name for which the Signature is to be configured. It displays the list of signatures included in the category and what action will be taken if signature is identified.

Click Signature Name to view the details of the Signature

Green check mark indicates that the Signature is enabled

Red Cross indicates that the Signature is disabled

Click Edit mark against the Signature to be configured

- Displays Policy name

- In Enabled field,

Select 'ON' to use signature in detection and/or prevention

In IDP mode, select Drop or Detect

Mode decides what action to take if the pattern matching to the Signature is found.

**Drop mode**

If any traffic that matches the signature is detected, Cyberoam logs the details, gives the alert to the Administrator, and automatically drops the packets that triggered IDP, resets the connection, and prevents the traffic to reach its destination.

**Detect mode**

If any traffic that matches the signature is detected, Cyberoam logs the details and gives alert to the Administrator, but does not take any action against the traffic and the connection proceeds to its intended destination.

Select 'OFF' to exclude signature from detection and/or prevention process

5. Click Save to save the settings

**Edit IDP Policy**

CCC Help L

**Edit IDP Policy**

Name\* lantowan\_strict

Description A Strict IDP policy for LAN to WAN Traffic

Category	Action	Status	Edit	
+	dns	-	✓	
+	finger	-	✓	
-	ftp	-	✓	
	FTP ADMw0rm ftp login attempt	Detect	✓	
	FTP .forward	-	✓	
	FTP .rhosts	-	✓	
	FTP CWD ~root at	-	✓	
	FTP CEL overflow	-	✓	
	FTP adm scan	-	✓	
	FTP iss scan	-	✓	
	FTP pass wh00t	-	✓	
	FTP passwd retrie	-	✓	
	FTP piss scan	-	✓	
	FTP saint scan	-	✓	
	FTP satan scan	-	✓	
	FTP serv-u directory transversal	Detect	✓	

**Edit IDP Rule**

Rule FTP ADMw0rm ftp login attempt

Policy lantowan\_strict

Enabled\* ON

IDP Mode\* Detect

Save Cancel

Done Internet

Save Cancel

**To update IDP policy**

1. Select **IDP → Policy → Manage** and click the policy you want to edit
2. Displays policy name
3. Displays policy description, modify if required
4. Displays list of signature categories.  
Green check mark against the Category indicates that the category is enabled  
Red Cross mark against the Category indicates that the category is disabled

Click Edit mark against the Category which you want to enable/disable. See '[To Enable/Disable Category](#)' for more details.

5. Click next to the Category name for which the Signature is to be configured. It displays the list of signatures included in the category and what action will be taken if signature is identified.

Click Signature Name to view the details of the Signature

Green check mark against the signature indicates that the signature is enabled for use

Red Cross mark against the signature indicates that the signature is disabled

Click Edit mark against the signature which you want to enable/disable. See [To configure individual Signature](#) for more details.

6. Click Save to save the updated details

IDP Policy Name	Description	Apply	Del
lantowan_strict	A Strict IDP policy for LAN to WAN Traffic	Apply	<input type="checkbox"/>
generalpolicy	Default IDP Policy	Apply	<input type="checkbox"/>

Category Name	Action	Enable	Edit
+ dns	-	✓	
+ finger	-	✓	
+ ftp	-	✓	
+ telnet	-	✓	
+ information	-	✓	
+ icmp	-	✓	
+ imap	-	✓	
+ dbms	-	✓	
+ sql rules	-	✓	
+ netbios	-	✓	
+ nntp	-	✓	
+ backdoor	-	✓	
+ pop	-	✓	
+ web access	-	✓	
+ smtp	-	✓	

Save Cancel

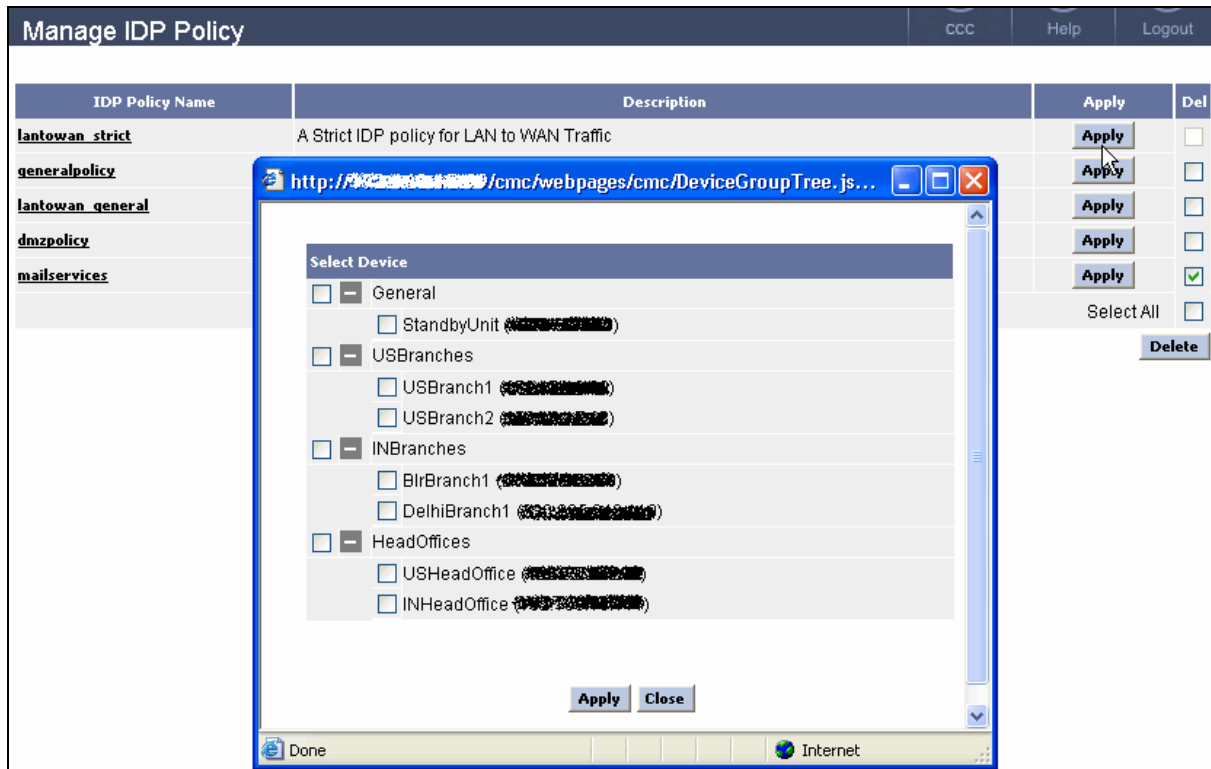
## Manage IDP Policy

Use

- [Update IDP policy](#)
- [Enable/Disable Category](#)
- [Configure individual Signature](#)
- [Delete Policy](#). Deleting IDP policy will delete from the Cyberoam Central Console and not from the devices.
- Assign IDP policy to a Device

## To assign IDP policy to a Device

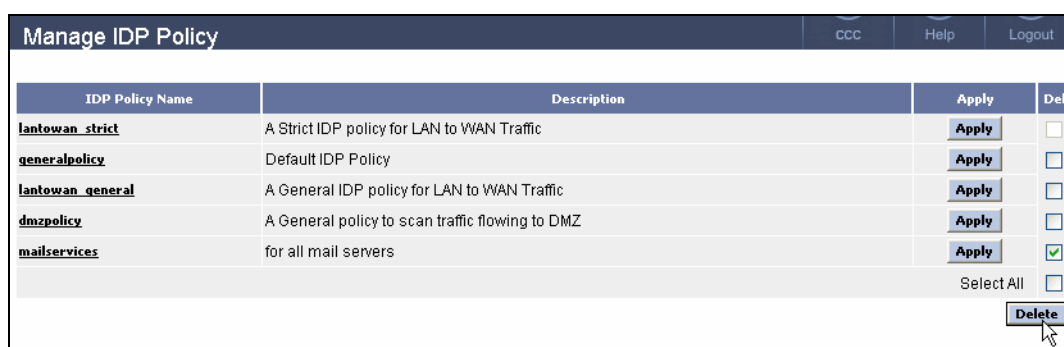
1. Select **IDP → IDP policy → Manage**
2. Click Apply against the IDP policy name. It opens a new page and displays group wise devices. Enable the check box against the group or device to which the IDP policy is to be added.
3. Click Apply. Applied will be displayed against the group/device, if the IDP policy is added successfully.



### To delete IDP Policy

1. Select **IDP → Policy → Manage IDP Policy** to view the list of policies
2. Click Del against the policy to be deleted OR
3. Click Select All to delete all the policies
4. Click Delete

Deleting IDP policy will delete from the Cyberoam Central Console and not from the devices.



## Custom Signatures

Custom signatures provide the flexibility to customize IDP for diverse network environments. Default signatures included in Cyberoam cover common attacks while custom signatures 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.

Create custom signature to define custom IDP signatures for your own network and use to allow or block specific traffic.

- [Create Custom Signature](#)
- [Manage Custom Signature](#)

### Create Custom Signature

Use to

- Create custom signature
- Update custom signature

#### To create custom signature

1. Select **IDP → Custom Signature → Create**
2. Enter custom signature name
3. Select Protocol
4. Enter Signature

Signature definition must begin with keyword followed by the value enclosed between the double quotes and must end with semicolon (;)

Format: Keyword:"value";

E.g. content:"USER JOHN";

If traffic with the content USER JOHN is detected, action defined in the policy will be taken.

5. Select Severity level of the signature. Severity level can be Warning, Minor, Moderate, Major, or Critical.
6. Select Default Mode. Mode decides what action to take if the pattern matching to the Signature is found.

Drop mode

If any traffic that matches the signature is detected, Cyberoam logs the details, gives the alert to the Administrator, and automatically drops the packets that triggered IDP, resets the connection, and prevents the traffic to reach its destination.

Detect mode

If any traffic that matches the signature is detected, Cyberoam logs the details and gives alert to the Administrator, but does not take any action against the traffic and the connection proceeds to its intended destination.

Select 'OFF' to exclude signature from detection and/or prevention process

The default mode selected will be applicable for all the IDP policies. You can override the default mode of the signature for the each IDP policy.

7. For each policy, set action to be taken if traffic matching to the signature is found.

8. Enter Description
9. Click create to create the signature

### To update custom signature

1. Select **IDP → Custom Signature → Manage** to view list of signatures
2. Displays custom signature name, modify if required
3. Displays Protocol, modify if required
4. Displays Signature

Signature definition must begin with keyword followed by the value enclosed between the double quotes and must end with semicolon (;)

Format: Keyword:"value";

E.g. content:"USER JOHN";

If traffic with the content USER JOHN is detected, action defined in the policy will be taken.

Refer to Appendix C – IDP - Custom Signature Syntax for more details on creating signature

5. Displays Severity level of the signature. Severity level can be Warning, Minor, Moderate, Major, or Critical.
6. Displays Default Mode. Mode decides what action to take if the pattern matching to the Signature is found, modify if required

#### Drop mode

If any traffic that matches the signature is detected, Cyberoam logs the details, gives the alert to the Administrator, and automatically drops the packets that triggered IDP, resets the connection and prevents the traffic to reach its destination.

#### Detect mode

If any traffic that matches the signature is detected, Cyberoam logs the details and gives alert to the Administrator, but does not take any action against the traffic and the connection proceeds to its intended destination.

Select 'OFF' to exclude signature from detection and/or prevention process

The default mode selected will be applicable for all the IDP policies. You can override the default mode of the signature for the each IDP policy.

7. Displays the action for each policy, modify if required.
8. Displays Description, modify if required
9. Click Save

The screenshot shows the 'Edit Custom Signature' dialog box. It contains the following fields and options:

- Custom Signature Name\***: ork
- Protocol\***: TCP (dropdown)
- Custom Rule\***: srcport:44;content:"www.ork.com";
- Severity\***: Warning (dropdown)
- Custom Signature Mode**:
  - Default Mode\***: Detect, Drop, Off (radio buttons, with 'Off' selected)
- Description**: (empty text area)
- Buttons**: Save, Cancel

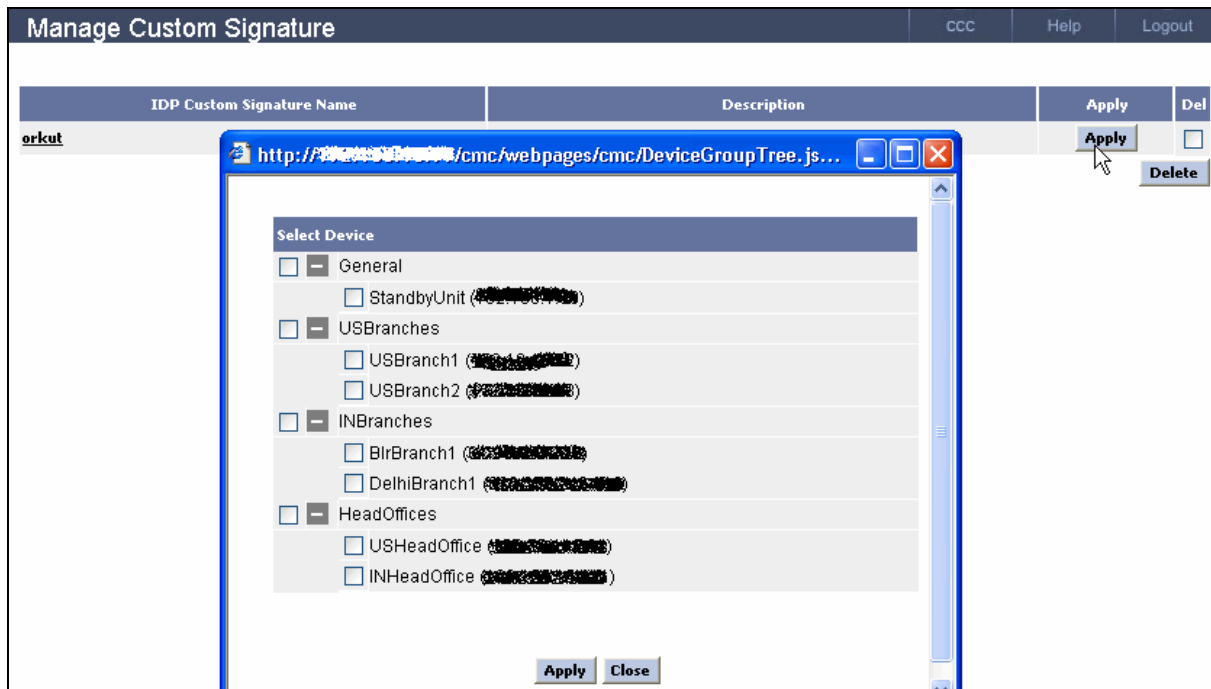
## Manage Custom Signature

Use to

- Update custom signature. Click the custom signature name to be update.
- Assign Signature to a Device
- Delete custom signature

### To assign IDP signature to a Device

1. Select **IDP → Custom Signature → Manage**
2. Click Apply against the Custom Signature name. It opens a new page and displays group wise devices. Enable the check box against the group or device to which the Custom Signature is to be added.
3. Click Apply. Applied will be displayed against the group/device, if the Custom Signature is added successfully.



### To delete custom signature

1. Select **IDP → Custom Signature → Manage** to view the list of custom signatures
2. Click Del against the signature to be deleted OR
3. Click Select All to delete all the signatures
4. Click Delete





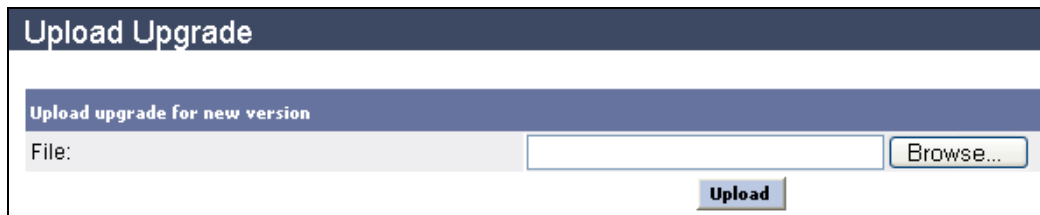
# Help

## Upload Upgrade

Once the upgraded version update file is obtained (CD or Downloaded), upload the new version file.

1. Select **Help → Upload Upgrade**
2. Type the file name with full path or select using 'Browse'
3. Click Upload

Once the upgrade file is uploaded successfully, log on to Console to upgrade the version. Refer Console guide for details.



## Licensing

You need a customer account to:

- register your Cyberoam Central Console appliance
- avail 8 X 5 support
- subscribe for 24 X 7 support

Select Help → Licensing to view the list of subscription modules. Screen shows licensing status of Appliances and subscription modules along with the subscription expiry date if subscribed.

Status - 'Registered' – Appliance registered

Status - 'Unregistered', – Appliance not registered

Status - 'Subscribed' - Module subscribed

Status - 'Unsubscribed' - Module not subscribed

Status - 'Trial' - Trial subscription

Status - 'Expired' - Subscription expired

### To create customer account/register Appliance

You need to create a user account to register appliance.

1. Select **Help → Licensing**
2. Click Register against Appliance
3. Displays Appliance Key and Appliance Model number
4. If you have already created an account, type your username and password to register appliance and go to step 12
5. Enter Email id. Account will be created with this email id and you will be able to access your

- account using this id.
6. Enter password for the account and confirm by re-typing.
  7. Enter name of the company under whose name appliance is to be registered
  8. Enter contact person name
  9. Enter complete address, phone number, Email Id & Fax number of the Company
  10. Enter secret question and answer related to your password. Question will be mailed in-case you forget password. If your answer matches, new password will be mailed.
  11. Configure for proxy server if HTTP Proxy Server is used to connect to Web
    - Click External Proxy server information
    - Enter HTTP proxy server setting (name or IP address) to connect to Cyberoam registration server
    - Enter port number if proxy server is running on the port than other than the default port (80)
    - Enter Username with which to log on to proxy server (if configured)
    - Enter Password (if configured)
  12. Click Register. This will create customer account and register the appliance.

### To subscribe add-on modules

- Customer has to procure a different license and subscribe for 24 X 7 Support
1. Select **Help → Licensing** to view the list of add-on modules
  2. Click Subscribe or Trial against the Module name which you want to register
  3. Displays Appliance key and model number
  4. Displays module name which will be registered
  5. Enter Email and password of your registered account
  6. Enter subscription key obtained from the sales person in-case you have purchased the license for the module
  7. Configure for proxy server if HTTP Proxy Server is used to connect to Web
    - Click External Proxy server Information
    - Enter HTTP proxy server setting (name or IP address) to connect to Cyberoam registration server
    - Enter port number if proxy server is running on the port than other than the default port (80)
    - Enter Username with which to log on to proxy server (if configured)
    - Enter Password (if configured)
  8. Click Subscribe or Trial depending on what you are registering

Add On Modules Subscription				
		CCC	Help	Logout
Modules	Subscription	Trial Subscription	Status	Expiration Date
CMC100 Appliance	-	-	Registered	-
24 x 7 Support	<a href="#">Subscribe</a>	-	Unsubscribed	-
8 x 5 Support	<a href="#">Subscribe</a>	-	Subscribed	Jun 04, 2008

### Add On Modules Subscription

#### Subscribe to 24 x 7 Support

Appliance Key	C015003503-2HVA206J
Appliance Model No	CMC100
Module	24 x 7 Support
Registered Email Id*	<input type="text"/>
Password*	<input type="password"/>
Subscription Key*	<input type="text"/> - <input type="text"/>

#### External Proxy Server Information