How To – Block Gmail Web Chat

Applicable Version: 10.00 onwards

Overview

Cyberoam allows you to block different Gmail applications/services with the help of Application Filter Policy. Applications in Gmail that can be controlled are listed below.

- Gmail Video Chat Streaming
- Gmail WebChat
- Gmail WebMail
- Gmail-Way2SMS WebMail

Scenario

Create an Application Filter Policy to block Gmail Web chat. The other Gmail services should be allowed.

Prerequisite

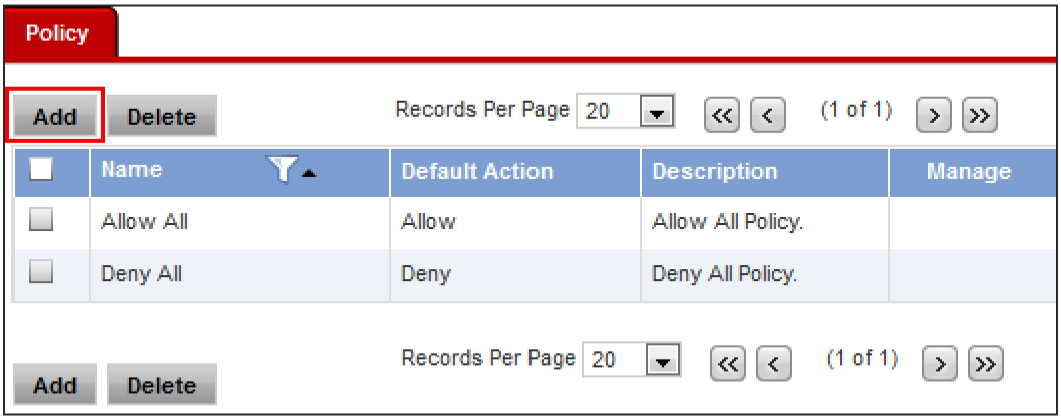
Web and Application Filter Module is subscribed.

Configuration

You can block Gmail Web Chat by following steps given below. Configuration is to be done from Web Admin Console using Administrator profile.

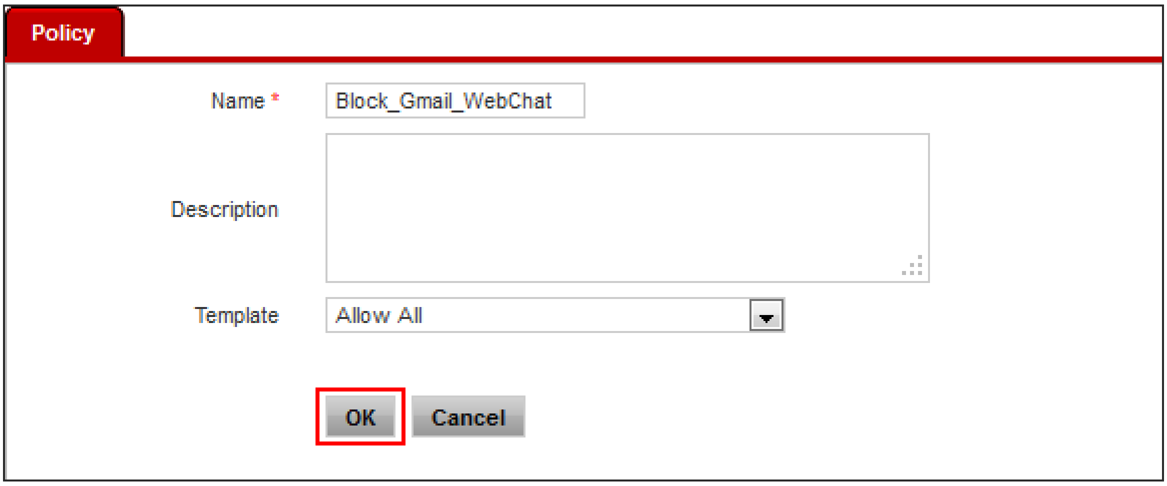
Step 1: Create Application Filter Policy

Go to **Application Filter** → **Policy** → **Policy** and click **Add** to create a new policy with parameters given below.



☐	Name	Default Action	Description	Manage
☐	Allow All	Allow	Allow All Policy.	
☐	Deny All	Deny	Deny All Policy.	

Parameters	Value	Description
Name	**Block_Gmail_Chat**	Specify a name to identify the Application Filter Policy
Template	**Allow All**	All the applications are allowed, but some defined categories are blocked



Name *	Block_Gmail_WebChat
Description	
Template	Allow All

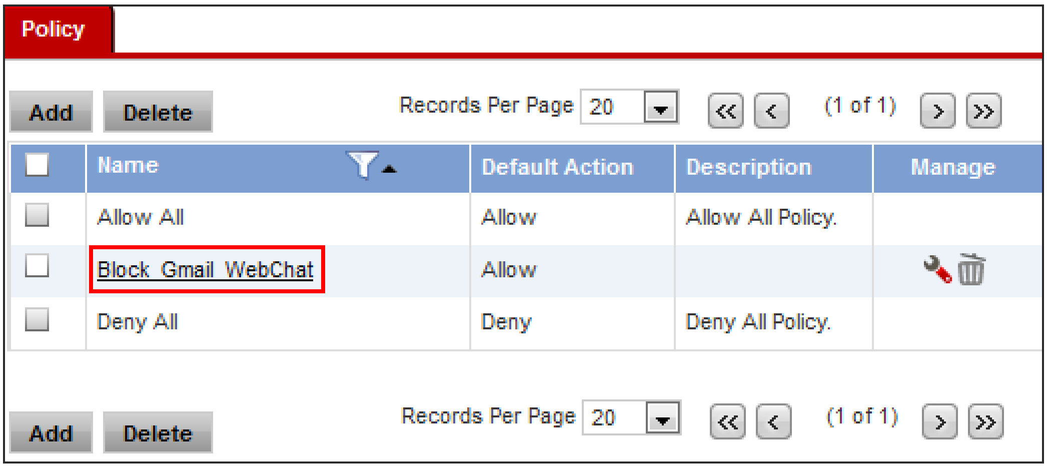
Click **OK** to create the policy.

Note:

Appliance is shipped with the following predefined policies for applications: Allow All and Deny All. These two predefined policies are immediately available for use until configured otherwise. You can also define custom policies to define different levels of access for different users to meet your organization's requirements.

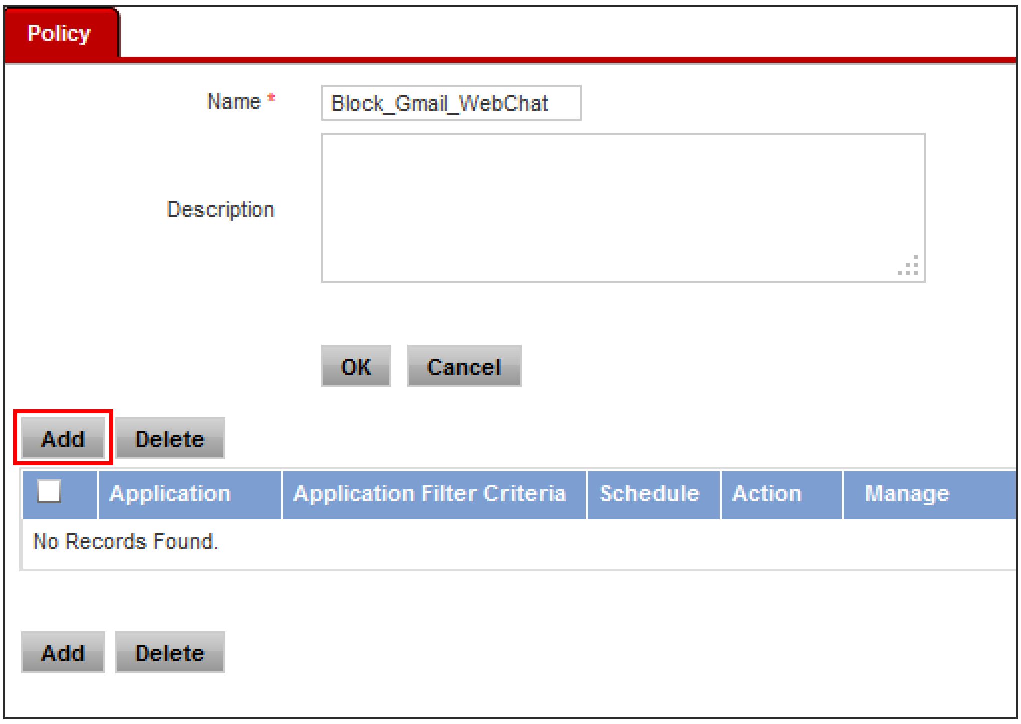
Step 2: Add Rules to Policy

Go to **Application Filter → Policy → Policy** and select the policy created in step 1.



□	Name	Default Action	Description	Manage
□	Allow All	Allow	Allow All Policy.	
□	Block_Gmail_WebChat	Allow		
□	Deny All	Deny	Deny All Policy.	

Click **Add** to add rules in the policy according to parameters given below.

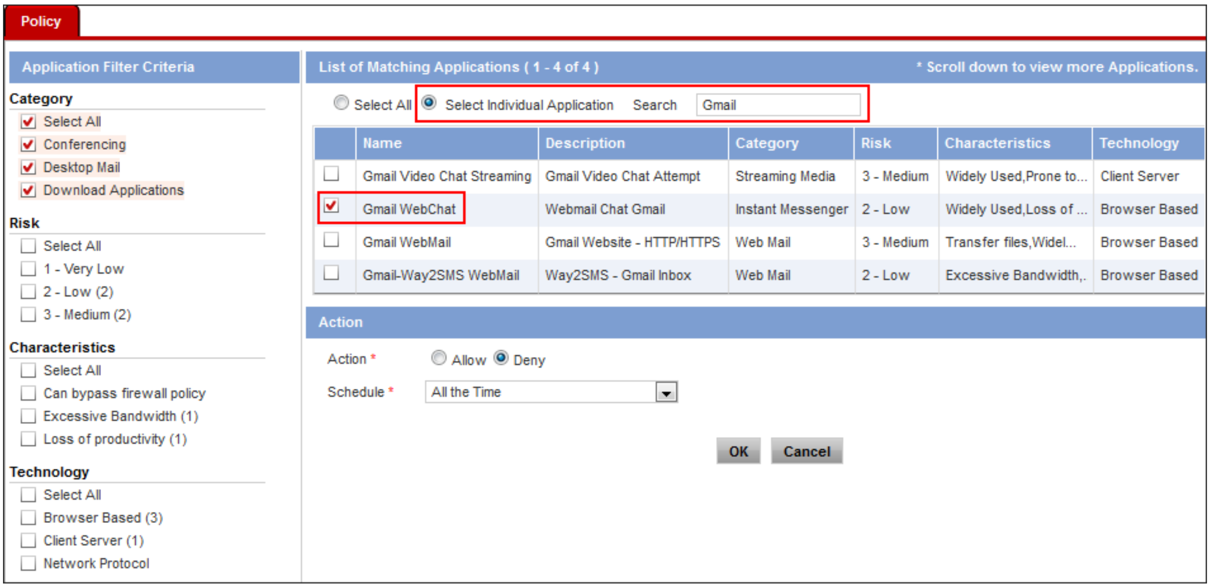


Name * Block_Gmail_WebChat

Description

□	Application	Application Filter Criteria	Schedule	Action	Manage
No Records Found.					

Parameter	Value	Description
Application Filter Criteria	**Select All**	Select the criteria upon which applications are to be selected
List of Applications	**Select Individual Application**	Based on the Application Filter Criteria, applications are listed. Select **Gmail WebChat**.
Action	**Deny**	Select the Action: Allow OR Deny.
Schedule	**All the time**	Select the Schedule from the list of Schedules available



Policy

Application Filter Criteria

Category
- ☑ Select All
- ☑ Conferencing
- ☑ Desktop Mail
- ☑ Download Applications

Risk
- □ Select All
- □ 1 - Very Low
- □ 2 - Low (2)
- □ 3 - Medium (2)

Characteristics
- □ Select All
- □ Can bypass firewall policy
- □ Excessive Bandwidth (1)
- □ Loss of productivity (1)

Technology
- □ Select All
- □ Browser Based (3)
- □ Client Server (1)
- □ Network Protocol

List of Matching Applications (1 - 4 of 4) * Scroll down to view more Applications.

○ Select All ● Select Individual Application Search Gmail

	Name	Description	Category	Risk	Characteristics	Technology
□	Gmail Video Chat Streaming	Gmail Video Chat Attempt	Streaming Media	3 - Medium	Widely Used,Prone to...	Client Server
☑	Gmail WebChat	Webmail Chat Gmail	Instant Messenger	2 - Low	Widely Used,Loss of ...	Browser Based
□	Gmail WebMail	Gmail Website - HTTP/HTTPS	Web Mail	3 - Medium	Transfer files,Widel...	Browser Based
□	Gmail-Way2SMS WebMail	Way2SMS - Gmail Inbox	Web Mail	2 - Low	Excessive Bandwidth,.	Browser Based

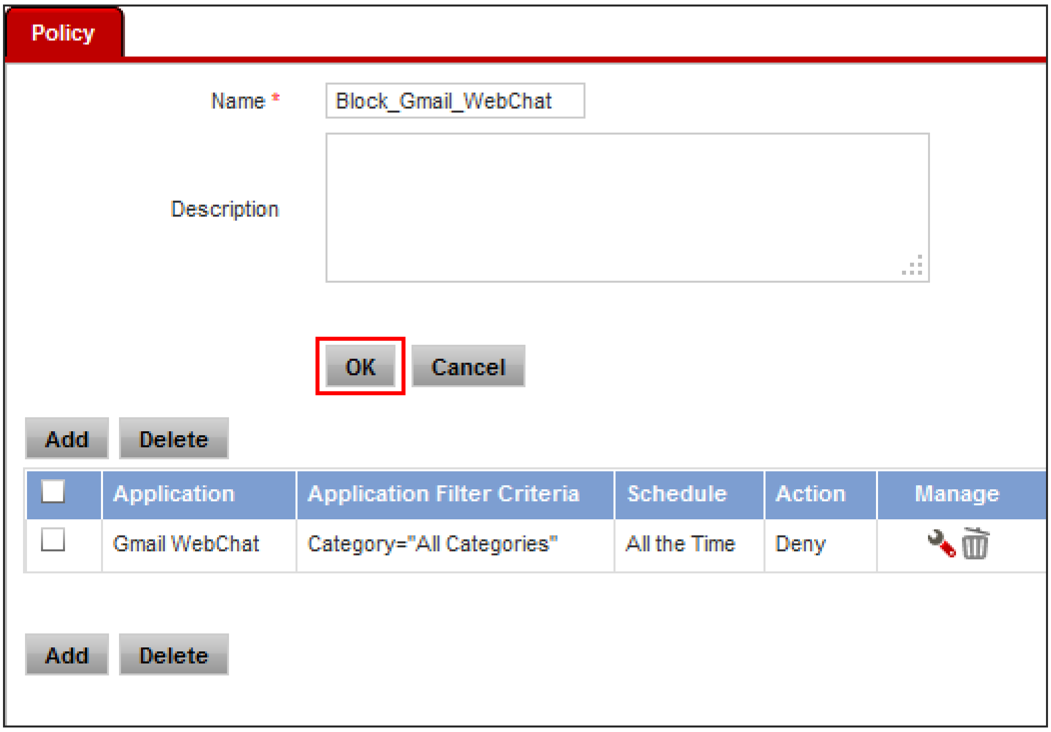
Action

Action * ○ Allow ● Deny

Schedule * All the Time

OK Cancel

Click **OK** to add rule to Block_Gmail_Chat policy.



Policy

Name * Block_Gmail_WebChat

Description

OK Cancel

Add Delete

□	Application	Application Filter Criteria	Schedule	Action	Manage
□	Gmail WebChat	Category="All Categories"	All the Time	Deny	

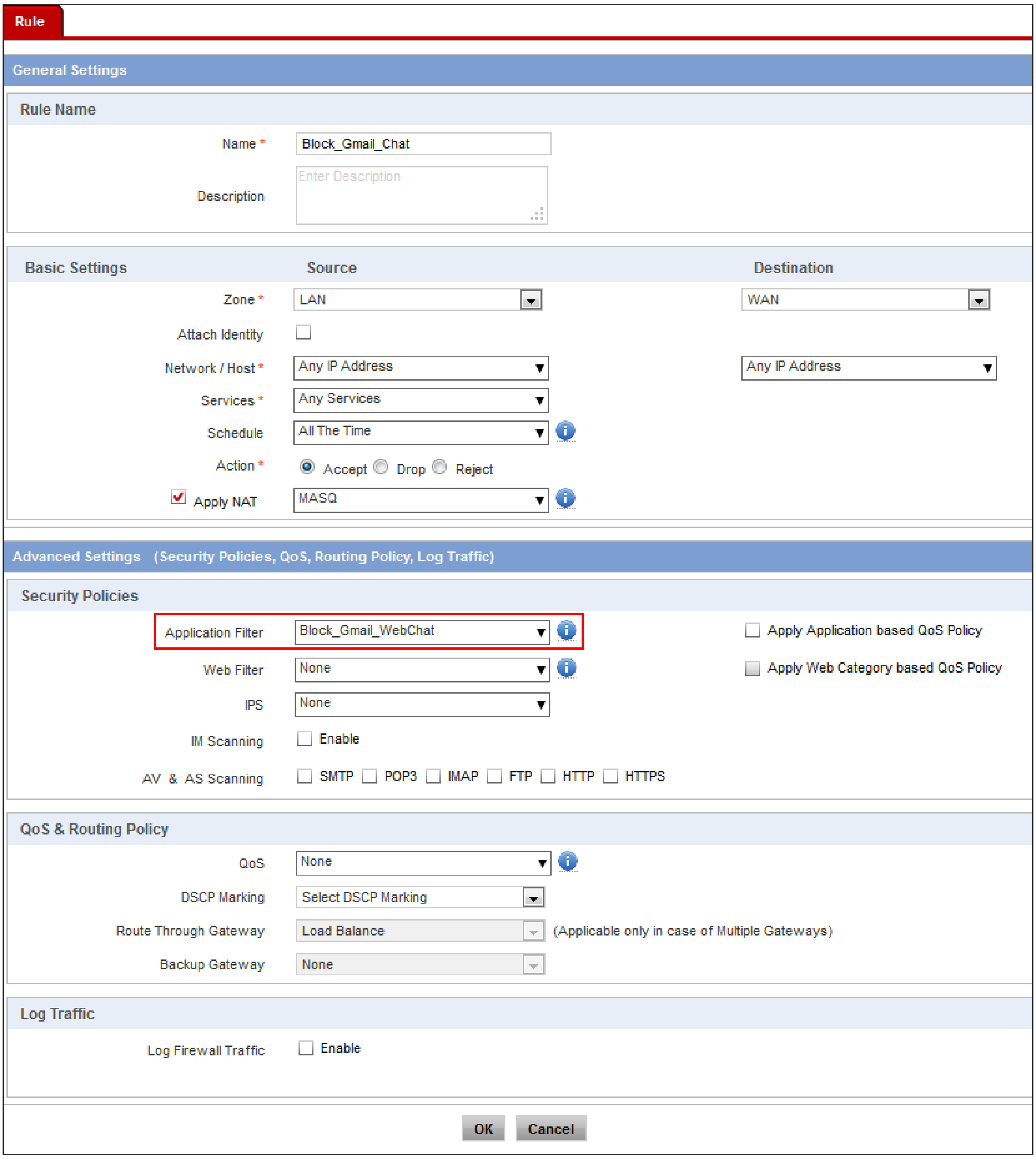
Add Delete

Click **OK** to save the policy.

Step 3: Apply Policy to Firewall Rule or User/User Group

Firewall Rule

You can apply the policy through a Firewall Rule such that it is applied on all traffic that hits on that rule. To create a Firewall Rule, go to **Firewall → Rule → Rule** and click **Add.** As shown below, apply the Policy created in step 1.



Rule

General Settings

Rule Name

Name * Block_Gmail_Chat

Description Enter Description

Basic Settings — Source — Destination

Zone * LAN — WAN

Attach Identity □

Network / Host * Any IP Address — Any IP Address

Services * Any Services

Schedule All The Time

Action * ● Accept ○ Drop ○ Reject

☑ Apply NAT MASQ

Advanced Settings (Security Policies, QoS, Routing Policy, Log Traffic)

Security Policies

Application Filter Block_Gmail_WebChat

□ Apply Application based QoS Policy

Web Filter None

□ Apply Web Category based QoS Policy

IPS None

IM Scanning □ Enable

AV & AS Scanning □ SMTP □ POP3 □ IMAP □ FTP □ HTTP □ HTTPS

QoS & Routing Policy

QoS None

DSCP Marking Select DSCP Marking

Route Through Gateway Load Balance (Applicable only in case of Multiple Gateways)

Backup Gateway None

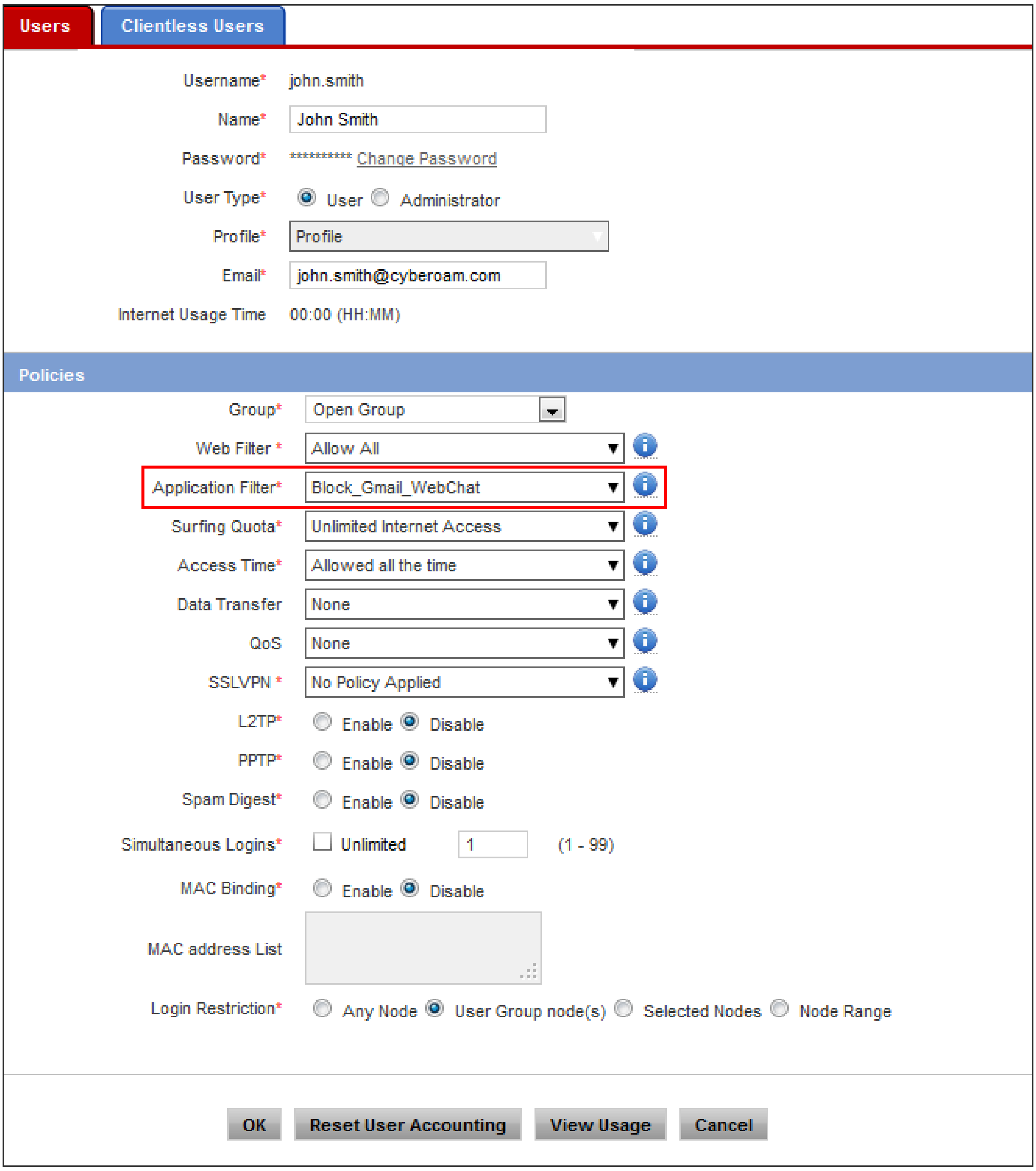
Log Traffic

Log Firewall Traffic □ Enable

Click **OK** to create the Firewall Rule.

User/User Group

You can apply the rule to individual users or user groups. Here, as an example we have applied the rule on a user named John Smith. To apply the policy on an individual user, go to Identity → Users → Users and click the user on whom policy is to be applied, i.e., John Smith. As shown below, apply the Policy created in step 1.



Username* john.smith

Name* John Smith

Password* ********** Change Password

User Type* ● User ○ Administrator

Profile* Profile

Email* john.smith@cyberoam.com

Internet Usage Time 00:00 (HH:MM)

Policies

Group* Open Group

Web Filter * Allow All

Application Filter* Block_Gmail_WebChat

Surfing Quota* Unlimited Internet Access

Access Time* Allowed all the time

Data Transfer None

QoS None

SSLVPN * No Policy Applied

L2TP* ○ Enable ● Disable

PPTP* ○ Enable ● Disable

Spam Digest* ○ Enable ● Disable

Simultaneous Logins* □ Unlimited 1 (1 - 99)

MAC Binding* ○ Enable ● Disable

MAC address List

Login Restriction* ○ Any Node ● User Group node(s) ○ Selected Nodes ○ Node Range

Click **OK** to apply policy on the user.