

UNIBOX

An Intelligent Network Controller

Knowledge Base:

Control Module



© Copyright 2013 Wifi-soft Solutions Pvt. Ltd. All rights reserved.

The information contained herein is subject to change without notice. This document contains proprietary information, which is protected by copyright. No part of this document may be photocopied, reproduced, or translated into another language without the prior written consent of Wifi-soft.

Publication Date

June 14, 2013

Applicable Products

The administration guide applies to the following products –

- Unibox U-50
- UniBox U-100
- UniBox U-200
- UniBox U-500
- UniBox U-1000

Disclaimer

WIFI-SOFT SOLUTIONS PRIVATE LIMITED MAKES NO WARRANTY OF ANY KIND WITH REGARD TO THIS MATERIAL, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.


Wifi-soft shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

The only warranties for Wifi-soft products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Wifi-soft shall not be liable for technical or editorial errors or omissions contained herein.

Wifi-soft assumes no responsibility for the use or reliability of its software on equipment that is not furnished by Wifi-soft.


1) How to set Date and time policy in Unibox?

- ✓ Open unibox dashboard in web browser.
- ✓ Navigate to policy section under control panel.
- ✓ Click on Date and time policy option from left pane.
- ✓ First we need to enable policy, click on enable policy checkbox and click on submit.

 **Control :: Date & Time**

Enable this policy

- ✓ Once the policy is enabled, create new date and time policy by clicking on “New Date and Time policy” option from left pane.

 **Control :: New Date & Time Policy**

Allow access to group of users based on date & time

New Date & Time Policy

Policy Name*
Group*

Days of week *

Every Day:
OR

Sunday: Monday: Tuesday: Wednesday: Thursday: Friday: Saturday:

Time of the day *

24 Hours:
OR

From e.g: 1-3,12-13

- ✓ Give name for the policy.
- ✓ Select group from drop down list on policy will be applied.
- ✓ Select days of week, can select Everyday or specific days of week.
- ✓ Mention time of the day, can select as 24 hours or specific time intervals at that time policy will get applied.
- ✓ Click on submit to save policy configuration settings.

2) How to set Relogin policy in Unibox?

- ✓ Open unibox dashboard in web browser.
- ✓ Navigate to policy section under control panel.
- ✓ Click on relogin option from left pane.

- ✓ First we need to enable policy, click on enable policy checkbox and click on submit.

Control :: Relogin

Enable this policy

- ✓ Once the policy is enabled, create new relogin policy by clicking on “Relogin policy” option from left pane.

Control :: New Relogin Policy

Set multiple session policy for a given day

New Relogin Policy

Policy Name*
Group*

Maximum Login

Maximum Login* (per day)

Degrade Bandwidth

Upload Bandwidth*
Download Bandwidth*

- ✓ Give name for the policy.
- ✓ Select group from drop down list on policy will be applied.
- ✓ Give maximum number limit.
- ✓ Mention degrade bandwidth options such as upload and download bandwidth.
- ✓ Click on submit to save policy configuration settings.

3) How to set Variable Bandwidth policy in Unibox?

- ✓ Open unibox dashboard in web browser.
- ✓ Navigate to policy section under control panel.
- ✓ Click on variable bandwidth option from left pane.
- ✓ First we need to enable policy, click on enable policy checkbox and click on submit.

Control :: Variable Bandwidth

Enable this policy

- ✓ Once the policy is enabled, create new variable bandwidth policy by clicking on “New variable bandwidth policy” option from left pane.

Control :: New Variable Bandwidth

Apply bandwidth control for a given group

New policy

Policy Name*
Group*

Degrade Bandwidth

Upload Bandwidth to* Kbps after* Minutes
Download Bandwidth to* Kbps after* Minutes

- ✓ Give name for the policy.
- ✓ Select group from drop down list on policy will be applied.
- ✓ Give bandwidth degrade restrictions.
- ✓ Click on submit to save policy configuration settings.

4) How to set Load balancing policy in Unibox?

- ✓ Open unibox dashboard in web browser.
- ✓ Navigate to policy section under control panel.
- ✓ Click on variable balancing option from left pane.

Control :: Load Balancing

Enable this policy

- ✓ First we need to enable policy, click on enable policy checkbox and click on submit.
- ✓ Once the policy is enabled, create new load balancing policy by clicking on “New load balancing policy” option from left pane.

Control :: New Load Balancing

Apply bandwidth restriction as per load

New policy

Policy Name*
Group*

Available Bandwidth

Upload Bandwidth* Mbps
Download Bandwidth* Mbps

- ✓ Give name for the policy.
- ✓ Select group from drop down list on policy will be applied.
- ✓ Mention available bandwidth for upload and download.
- ✓ Click on submit to save policy configuration settings.

5) How to set fair usage policy in Unibox?

- ✓ Open unibox dashboard in web browser.
- ✓ Navigate to policy section under control panel.
- ✓ Click on fair usage option from left pane.

Control :: Fair Usage

Enable this policy

- ✓ First we need to enable policy, click on enable policy checkbox and click on submit.
- ✓ Once the policy is enabled, create new fair usage policy by clicking on “New fair usage policy” option from left pane.

 **Control :: New Fair Usage Policy**

Apply bandwidth control to group of users based on data usage

Policy Name*
Group*

Maximum Data Usage

Maximum Data Usage*

Timeframe for Data Usage

Consider data usage within

Degrade Bandwidth

Upload Bandwidth to*
Download Bandwidth to*

Apply policy to concurrent users

- ✓ Give name for the policy.
- ✓ Select group from drop down list on policy will be applied.
- ✓ Mention maximum data usage. Select data size from drop down list.
- ✓ Mention timeframe for data usage, select data size from drop down list.
- ✓ Mention degrades bandwidth for upload and download.
- ✓ If you want to apply this policy for the concurrent users then tick check box for the same.
- ✓ Click on submit to save policy configuration settings.

6) How to set data rate in bandwidth control?

- ✓ Open unibox dashboard in web browser
- ✓ Navigate to bandwidth control section under control TAB.
- ✓ First create new data rule. Click on New rule from left pane.

 **Control :: New Rule**



Please define Data Rate before creating rule. Click the button to define Data Rate

- ✓ Mention total upload rate.

Control :: Data Rate

 Configuration saved successfully

Edit Data Rate

Total Upload Rate *	<input type="text" value="512"/>	<input type="text" value="Kbps"/>
Total Download Rate *	<input type="text" value="3000"/>	<input type="text" value="Kbps"/>
Low Data Rate *	<input type="text" value="10"/>	% to 100 %
Average Data Rate *	<input type="text" value="20"/>	% to 100 %
High Data Rate *	<input type="text" value="30"/>	% to 100 %
Very High Data rate *	<input type="text" value="40"/>	% to 100 %


- ✓ Mention Download rate.
- ✓ Mention low, average, high and very high rate in terms of percentage but the sum of all rate should be equal to 100.
- ✓ Click on submit to save data rate.
- ✓ Click on New rule.
- ✓ Give name for the rule.
- ✓ Select traffic direction option from drop down list.
- ✓ There are two types of Rules
 - **Simple:** It is applied on the selected application from drop down list.

Control :: New Rule

Add New Rule

Rule Name *	<input type="text" value="Http"/>
Traffic Direction *	<input type="text" value="To WAN"/>
<input checked="" type="radio"/> Simple	<input type="radio"/> Advance
Application *	<input type="text" value="http"/>
Priority *	<input type="text" value="High"/>

- **Advanced:** Here you can mention source and destination IP addresses with port number to control flow of data, Select type of transmission protocol.

 **Control :: New Rule**



Add New Rule

Rule Name *

Traffic Direction *

Simple **Advance**

Source IP Port

Destination IP Port


Protocol

Priority *

- ✓ Select priority from drop down list.
- ✓ Click on submit to save the configuration changes.

7) How to delete all data rules in unibox?

- ✓ Open unibox dashboard in web browser.
- ✓ Navigate to bandwidth control section under control TAB.

 **Control :: Delete All Rules**



Are you sure you want to delete all Rules? ?

- ✓ Click on delete all data rules from left pane.


 **Control :: Delete All Rules**

 **Rules deleted successfully.**


- ✓ All rules will be deleted.

8) How to apply URL blocking or content filter feature in Unibox?

- ✓ Open unibox dashboard in web browser.
- ✓ Navigate to content filter section under control TAB.
- ✓ To enable content filter make sure that you should enable proxy settings.
- ✓ Go in tools, caching proxy and enable proxy.

 **Control :: Content Filter** ?

Please enable proxy before enabling content filter. Click on the button to enable proxy

 **Tools :: Caching / Proxy**


Proxy Settings

Enable Proxy

Enable Caching

Cache Timeout*

Cache Limit*


 **Control :: Content Filter**

Configure Content Filter

Enable Content Filter

Redirect URL*

- ✓ Tick check box to enable content filter.
- ✓ Mention redirection URL.
- ✓ Click on submit to enable.
- ✓ Click on manage domain option from left pane to block URL's by selecting categorized groups.

 **Control :: Manage Domains**

Configure Content Filter Domains

<input type="checkbox"/> Abortion	<input type="checkbox"/> Advertisements	<input type="checkbox"/> Adult	<input type="checkbox"/> Aggressive
<input checked="" type="checkbox"/> Alcohol	<input checked="" type="checkbox"/> Anti Spyware	<input type="checkbox"/> Arjel	<input type="checkbox"/> Art Nudes
<input type="checkbox"/> Astrology	<input checked="" type="checkbox"/> Audio-Video	<input type="checkbox"/> Bank	<input type="checkbox"/> Banking
<input type="checkbox"/> Beer/Liquor Info	<input checked="" type="checkbox"/> Beer/Liquor Sale	<input type="checkbox"/> Blog	<input type="checkbox"/> Books

<input type="checkbox"/> Social Networks	<input type="checkbox"/> Sport News	<input type="checkbox"/> Sports	<input type="checkbox"/> Spyware
<input type="checkbox"/> Tobacco	<input type="checkbox"/> Update Sites	<input type="checkbox"/> Vacations	<input type="checkbox"/> Verisign
<input type="checkbox"/> Violence	<input type="checkbox"/> Virus Infected	<input type="checkbox"/> Warez	<input type="checkbox"/> Weapons
<input type="checkbox"/> Weather	<input type="checkbox"/> Webmail	<input type="checkbox"/> Whitelist	

- ✓ Click on submit to save configuration.

9) How to add or remove URL's to block list?

- ✓ Open unibox dashboard in web browser.
- ✓ Navigate to content filter section under control TAB.
- ✓ Click on Exceptions option from left pane.
- ✓ **To block URL:**

The screenshot shows the 'Control :: Exceptions' page. At the top, there is a title bar with a warning icon and a question mark. Below it is a table with two columns: '# Domain' and 'Action'. The table is currently empty, with the text 'No Domain found' centered below it. Below the table is a 'Delete Selected' button. Underneath is the 'Add Exception' section, which includes a 'Domain *' text box containing 'www.facebook.com', an 'Action' dropdown menu set to 'Add To Block List', and a 'Submit' button.

- Mention URL in Domain textbox and take action selecting “Add to block list” from drop down list.

- ✓ **To Remove URL from blocked list:**

The screenshot shows the 'Control :: Exceptions' page after a successful update. At the top, there is a title bar with a warning icon and a question mark. Below it is a green checkmark icon followed by the text 'Configuration saved successfully'. Below this is a table with two columns: '# Domain' and 'Action'. The table contains one entry: a checked checkbox in the first column, '1' in the second column, 'www.facebook.com' in the third column, and 'add' in the fourth column. Below the table is a 'Delete Selected' button. Underneath is the 'Add Exception' section, which includes a 'Domain *' text box containing 'www.youtube.com', an 'Action' dropdown menu set to 'Remove From Block List', and a 'Submit' button.

- ✓ Mention URL in domain textbox and take action selecting “Remove from blocked list” from drop down list.
- ✓ Click on submit to save changes made.

10) How to block torrents in Unibox?

- ✓ Open unibox dashboard in web browser.
- ✓ Navigate to traffic analysis section under control panel.
- ✓ Enable Traffic analysis by ticking check box, click on submit.
- ✓ Once traffic analysis is enabled, click on add rule to set rules.
- ✓ Select the type of traffic you want to block from drop down list.
- ✓ Once the type is selected, select rule from drop down list.
- ✓ Give name for rule.

Control :: Configurations



Enable Traffic Analysis

Select Category: P2P

Select Rule: BitTorrent

Rule Name*: BitTorrent (Maximum 10 alphanumeric characters)

Protocol Name:

Source IP:

Source Port:

Destination IP:

Destination Port:

Actions

Email

Restrictions

Upload Speed: Kbps

Download Speed: Kbps

Max Upload: KB

Max Download: KB

Session Timeout: Seconds

Idle Timeout: Seconds

Category	Rule Name	Protocol	Source IP	Source Port	Destination IP	Destination Port	Action	Delete
P2P	Gnutella	-	-	-	-	-	-	<input type="button" value="Delete"/>

- ✓ Give protocol name, mention source port, source IP, Destination port, destination IP.
- ✓ Select the actions, if you want notification of traffic analysis then mention mail ID.
- ✓ If you want to restrict traffic, then mention upload speed, download speed, max upload & download Session timeout and idle timeout.
- ✓ Click on submit to save rule.

11) How to block specific traffic in unibox?

- ✓ Open unibox dashboard in web browser.
- ✓ Navigate to traffic analysis section under control TAB.
- ✓ Enable Traffic analysis by ticking check box, click on submit.
- ✓ Once traffic analysis is enabled, click on add rule to set rules.

There are various types of traffic that can be blocked under unibox:

- ✓ To block MAIL traffic:
 - ✓ Select category as Mail from drop down list.
 - ✓ Select the type of mailing protocol you want to block (Ex. POP3 or IMAP).

Control :: Configurations

Enable Traffic Analysis

Select Category

Select Rule

Rule Name* (Maximum 10 alphanumeric character)

Protocol Name

Source IP

Source Port

Destination IP

Destination Port

Actions

Email

Restrictions

Upload Speed Kbps

Download Speed Kbps

Max Upload KB

Max Download KB

Session Timeout Seconds

Idle Timeout Seconds

- ✓ These rules are predefined, if you want to add new rule then select option as custom rule. Select protocol name and configure rest of the settings.

Control :: Configurations

Enable Traffic Analysis

Select Category

Select Rule

Rule Name*

Protocol Name

Source IP

Source Port

Destination IP

Destination Port

Control :: Configurations

Enable Traffic Analysis

Select Category

Select Rule

Rule Name*

Protocol Name

Source IP

Source Port

Destination IP

Destination Port

- ✓ Click on submit to save rule.
- ✓ To block General Traffic:
 - ✓ General rule is categorized in to four types naming FTP, SSH, HTTP and custom rule.
 - ✓ To block FTP traffic:

Control :: Configurations

Enable Traffic Analysis

Select Category

Select Rule

Rule Name*

Protocol Name

Source IP

Source Port

Destination IP

Destination Port

- Select FTP from drop down list.
- Give rule name and protocol name, destination port is predefined.
- Configure rest settings and click on submit to save FTP rule.
- To block SSH traffic:
 - This is predefined rule with rule name, protocol and destination port.

Enable Traffic Analysis

Submit

Add Rule

Select Category: General

Select Rule: SSH

Rule Name*: SSH (Maxim)

Protocol Name: tcp

Source IP:

Source Port:

Destination IP:

Destination Port: 22

- Configure rest settings and click on submit to save SSH rule.
- To block HTTP traffic:

Enable Traffic Analysis

Submit

Add Rule

Select Category: General

Select Rule: HTTP

Rule Name*: HTTP

Protocol Name: tcp

Source IP:

Source Port:

Destination IP:

Destination Port: 80

- This is predefined rule with rule name, protocol and destination port.
- Configure rest settings and click on submit to save HTTP rule.
- Block general traffic configuring custom rule:

Enable Traffic Analysis

Select Category

Select Rule

Rule Name*

Protocol Name

Source IP

Source Port

Destination IP

Destination Port

- This is not predefined rule, select protocol for rule, port number.
- Configure rest settings and click on submit to save custom rule.

✓ To block gaming traffic:

Enable Traffic Analysis

Select Category

Select Rule

Rule Name*

Protocol Name

Source IP

Source Port

Destination IP

Destination Port

- This is predefined rule with rule name, protocol and destination port.
- Configure rest settings and click on submit to save CS rule.

▪ To block gaming traffic by setting rule:

Enable Traffic Analysis

Select Category

Select Rule

Rule Name*

Protocol Name

Source IP

Source Port

Destination IP

Destination Port

- This is not predefined rule, select protocol for rule, port number.
- Configure rest settings and click on submit to save custom rule.

✓ To block P2P traffic:

Enable Traffic Analysis

Select Category

Select Rule

Rule Name*

Protocol Name

Source IP

Source Port

Destination IP

Destination Port

- All the rules are predefined with rule name, protocol and destination port.
- Configure rest settings and click on submit to save rule.

✓ To block VOIP traffic:

Enable Traffic Analysis

Select Category

Select Rule

Rule Name*

Protocol Name

Source IP

Source Port


Destination IP

Destination Port

- This is predefined rule with rule name, protocol and destination port.
- Configure rest settings and click on submit to save RTP (Real time transport protocol) rule.

12) How to check traffic analysis reports?

- ✓ Open unibox dashboard in web browser.
- ✓ Navigate to policy section under control panel.
- ✓ Click on the reports option from left pane.
- ✓ Click on the name of rule to view the traffic analysis details.

 **Control :: Reports** 

Traffic Reports Search

Username	<input type="text"/>	Rule	Select ▼	Days	Select ▼	<input type="button" value="SEARCH"/>
----------	----------------------	------	----------	------	----------	---------------------------------------

Today's Summary

#	Rule	Total Users
1	P2P_BitTorrent	7