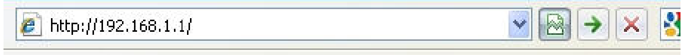
How to set up access control for website blocking on T Router (older green UI)?

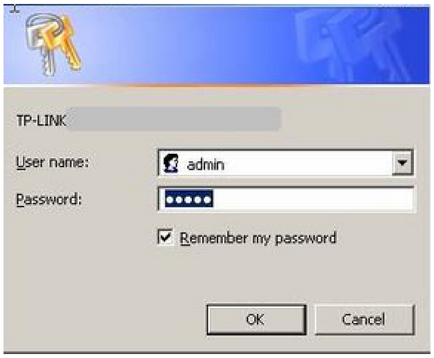
This Article Applies to:

TP-Link wireless N and Dual-band Routers provide convenient internet **Access Control** function.You can flexibly combine the **Host List**, **Target List** and **Sche** hosts.This document introduce how to set up website blocking on our wireless routers and we take TL-WR1043ND as example.

Step 1: Log in to your router's web management page.
Open the web browser and type the IP address of the router (default is **192.168.0.1** or **192.168.1.1**) or**http://tplinklogin.net** into the address bar and then Pre


http://192.168.1.1/

When you are prompted, enter the TL-WR1043ND´s username and password (the default username and password are both **admin**)

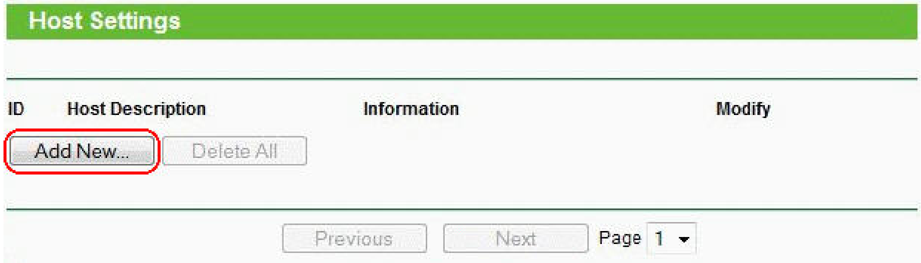

TP-LINK

User name: admin

Password: •••••

☑ Remember my password

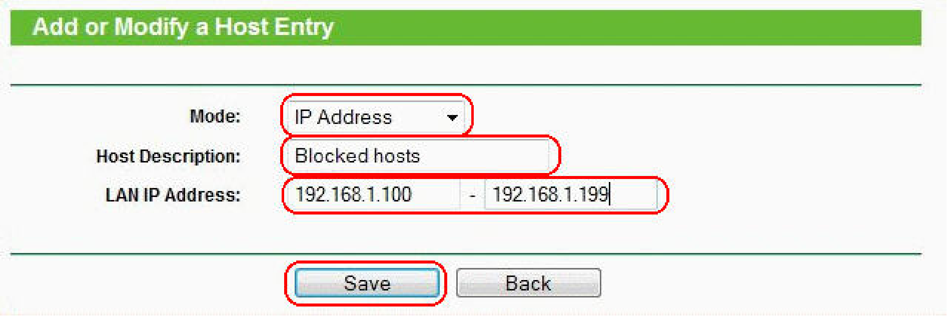
Step 2:
Go to **Access Control-Host**,then click "**Add New...**"


Host Settings

ID	Host Description	Information	Modify

Select "IP Address", then enter a short description for the host rule you want to define in the "Host Description:" box. Enter the IP address range on your netw

In this example,the router TL-WR1043's LAN IP address is 192.168.1.1,IP Range is 192.168.1.100~192.18.1.199.We are going to set up rules to block google a no restriction to any other websites.



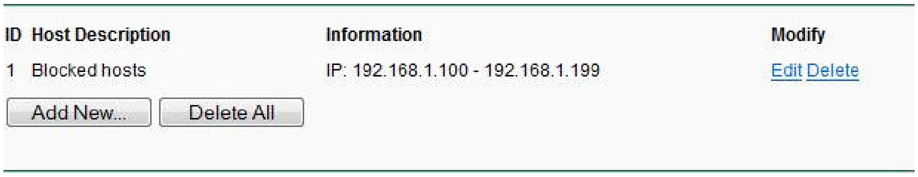
Add or Modify a Host Entry

Mode: IP Address

Host Description: Blocked hosts

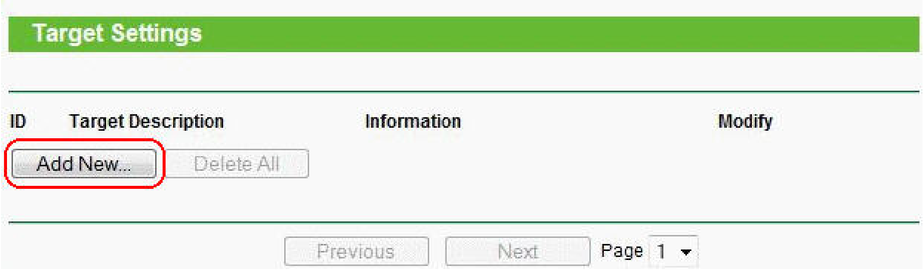
LAN IP Address: 192.168.1.100 - 192.168.1.199

Click "Save" - the new Host rule will now show up on the "Host Settings" page



ID	Host Description	Information	Modify
1	Blocked hosts	IP: 192.168.1.100 - 192.168.1.199	Edit Delete

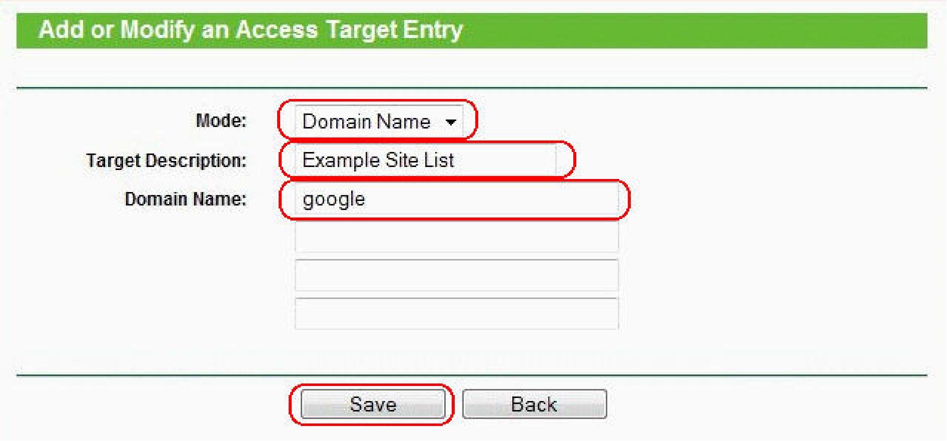
Step 3: Go to **Access Control -> Target**, then click "Add New..."



Target Settings

ID	Target Description	Information	Modify

Select "Domain Name" in the "Mode:" box, then enter a brief description of the rule you are setting up. In the "Domain Name:" box(es), enter the keywords you v to be full web addresses such as www.google.com - simply entering "google" will set the rule to block ANY domain name that contains the word "google")



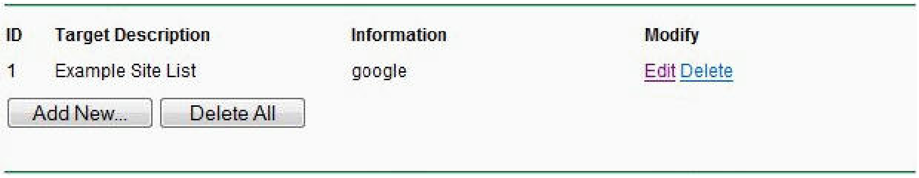
Add or Modify an Access Target Entry

Mode: Domain Name

Target Description: Example Site List

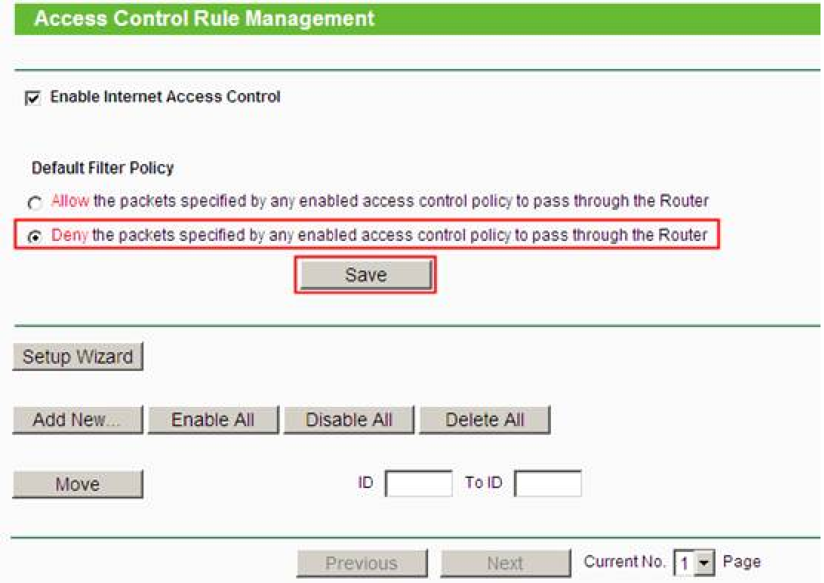
Domain Name: google

Click "Save" - the new Target rule will now show up on the "Target Settings" page



ID	Target Description	Information	Modify
1	Example Site List	google	Edit Delete

Step 4: Go to **Access Control -> Rule** page and tick "Enable Internet Access Control", then select the option " **Deny the packets specified by any enabled ac Router**" (if this is set to the "Allow" option, all websites other than ones you have set Host/Target rules for will be blocked), then click "Save".



Access Control Rule Management

☑ Enable Internet Access Control

Default Filter Policy

○ Allow the packets specified by any enabled access control policy to pass through the Router

● Deny the packets specified by any enabled access control policy to pass through the Router

Under **Access Control -> Rule**, click "Add New...", then enter a brief description of the rule in the "Rule Name:" box

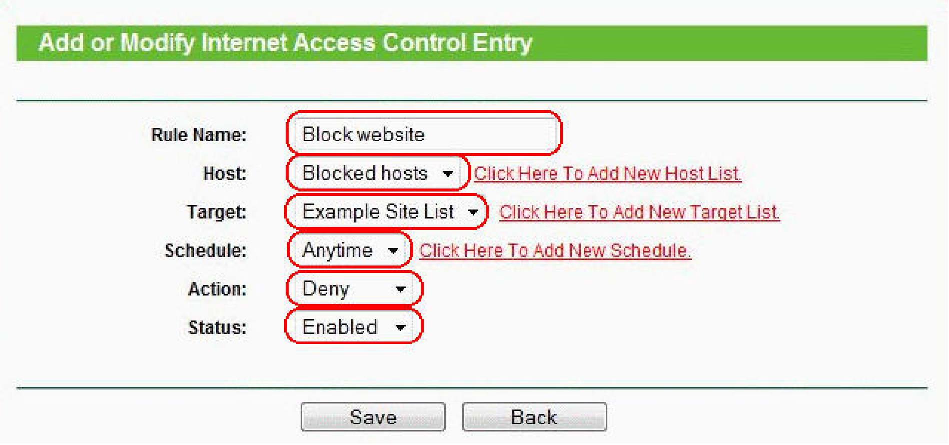
In the "Host:" box, select the Host rule you defined in **Step 2**

In the "Target:" box, select the target rule you defined in **Step 3**

In the "Schedule:" box, select "Anytime" (this will make the rule always active)

In the "Action:" box, select "Deny"

In the "Status:" box, select "Enabled"

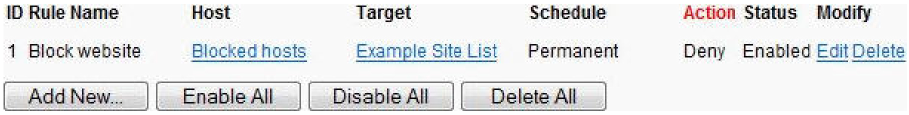


Add or Modify Internet Access Control Entry

Rule Name:	Block website
Host:	Blocked hosts
Target:	Example Site List
Schedule:	Anytime
Action:	Deny
Status:	Enabled

Click Here To Add New Host List.
Click Here To Add New Target List.
Click Here To Add New Schedule.
Save
Back

Click "Save" - the new Access Control rule will now show up on the "Access Control Rule Management" page .



ID	Rule Name	Host	Target	Schedule	Action	Status	Modify
1	Block website	Blocked hosts	Example Site List	Permanent	Deny	Enabled	Edit Delete

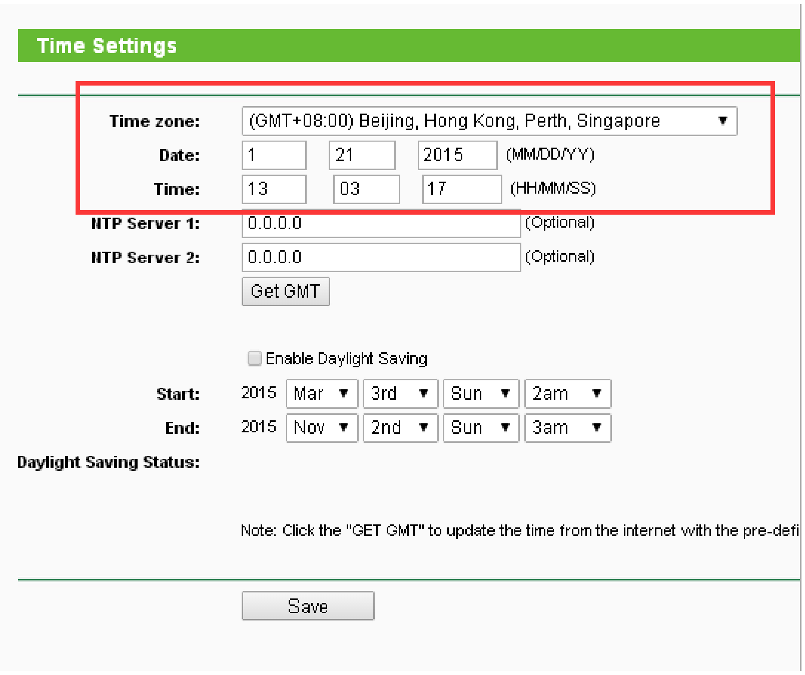
Step 5: To test the rule, try to browse to the site you have blocked from a host PC in the IP address range you defined in the Host rule in **Step 1** (for instance, h blocked, and your web browser will report that the site/server cannot be found.

Note:

A) If you want to block certain websites not all the time,but certain period,you may configure the Schedule under **Access Control-Schedule**.

Since Schedule rules are based on the router's time,please check the **Time Settings** on the router first,make sure it has the correct time zone and time .

1.Go to **System Tools-Time Settings** to check the time settings:



Time Settings

Time zone: (GMT+08:00) Beijing, Hong Kong, Perth, Singapore ▼

Date: 1 / 21 / 2015 (MM/DD/YY)

Time: 13 / 03 / 17 (HH/MM/SS)

NTP Server 1: 0.0.0.0 (Optional)

NTP Server 2: 0.0.0.0 (Optional)

Get GMT

□ Enable Daylight Saving

Start: 2015 Mar ▼ 3rd ▼ Sun ▼ 2am ▼

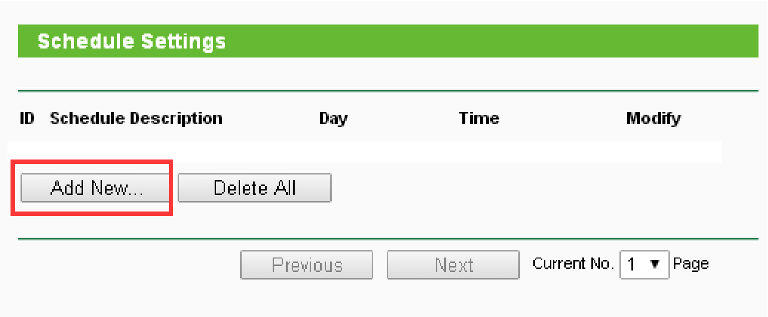
End: 2015 Nov ▼ 2nd ▼ Sun ▼ 3am ▼

Daylight Saving Status:

Note: Click the "GET GMT" to update the time from the internet with the pre-defi

Save

2.Go to **Access Control-Schedule**,click **Add New** .



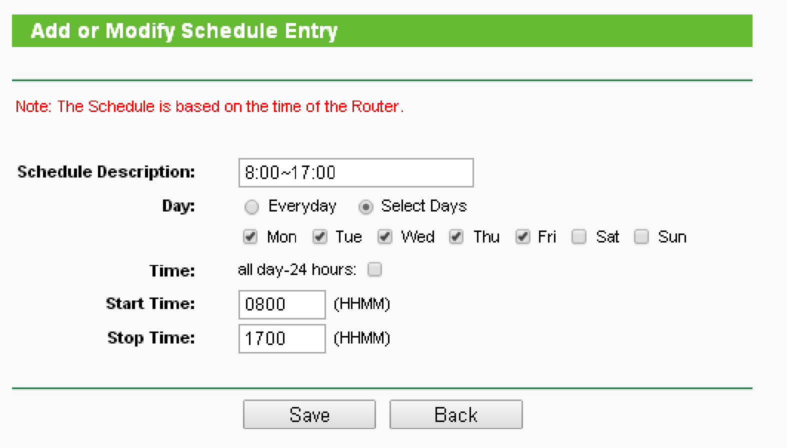
Schedule Settings

ID	Schedule Description	Day	Time	Modify

Add New... Delete All

Previous Next Current No. 1 ▼ Page

3.Create the rule according to your requirement.In my example,I selected Monday to Friday,8:00 Am to 5 Pm.



Add or Modify Schedule Entry

Note: The Schedule is based on the time of the Router.

Schedule Description: 8:00~17:00

Day: ○ Everyday ● Select Days

☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri □ Sat □ Sun

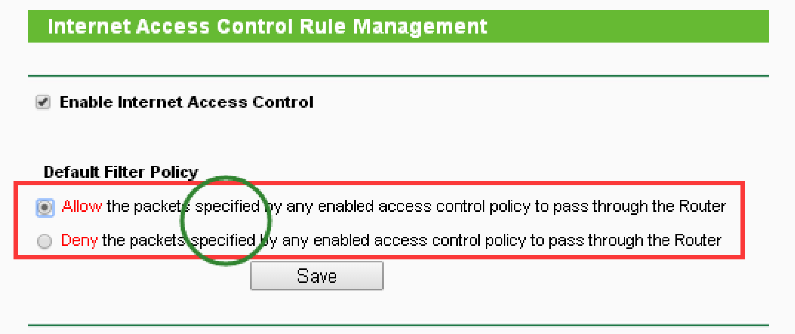
Time: all day-24 hours: □

Start Time: 0800 (HHMM)

Stop Time: 1700 (HHMM)

Save Back

B) For different models, the **Default Filter Policy/Rules** could be different. Please pay attention to each word of the rule .



Internet Access Control Rule Management

☑ Enable Internet Access Control

Default Filter Policy

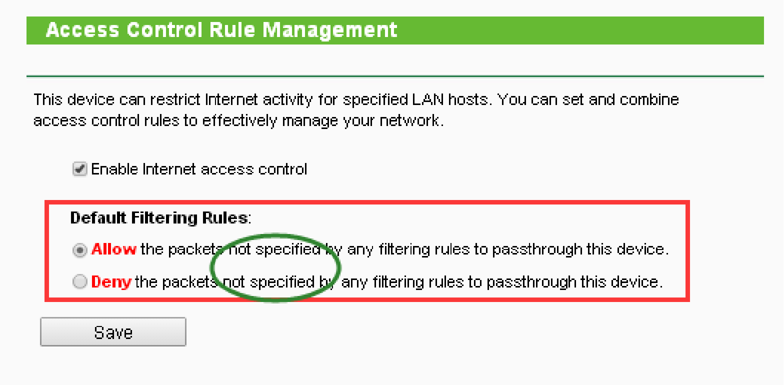
● Allow the packets specified by any enabled access control policy to pass through the Router

○ Deny the packets specified by any enabled access control policy to pass through the Router

Save

Under this **Default Filter Policy**,if we choose "Allow the packets specified by any enabled access control policy to pass through the Router",that means by de created rules to use internet.

If we choose "Deny the packets specified by any enabled access control policy to pass through the Router",that means by default it allow internet to all device internet.



Access Control Rule Management

This device can restrict Internet activity for specified LAN hosts. You can set and combine access control rules to effectively manage your network.

☑ Enable Internet access control

Default Filtering Rules:

● **Allow** the packets not specified by any filtering rules to passthrough this device.

○ **Deny** the packets not specified by any filtering rules to passthrough this device.

Under this **Default Filtering Rules**,if we choose "Allow the packets not specified by any enabled access control policy to pass through the Router",that means will only Block the created rules to use internet.

If we choose "Deny the packets not specified by any enabled access control policy to pass through the Router",that means by default it blocks all internet,anc internet.

Get to know more details of each function and configuration please go to Download Center **to download the manual of your product.**

Is this faq useful?

Your feedback helps improve this site.

Yes No

User Application

About Us
Corporate Profile
Contact Us
Privacy Policy

Press
News
Awards

Where to Buy
Channel Distributors
Retail Distributors
Retailers

Partners
Partner Program
Training & Certifications

Follow Us

United Arab Emirates / English