How to block access to specific IP addresses

Please note: Accessing your modem’s configuration pages does not require Internet connection as these pages are stored inside your modem. Your computer just needs to be connected to the modem.

- Open your Internet browser e.g. Internet Explorer, Edge, Firefox, Chrome, Safari, etc. and enter http://192.168.1.1 in the **address bar**:
- When prompted type in the Username and Password then click on the “Log In” button.

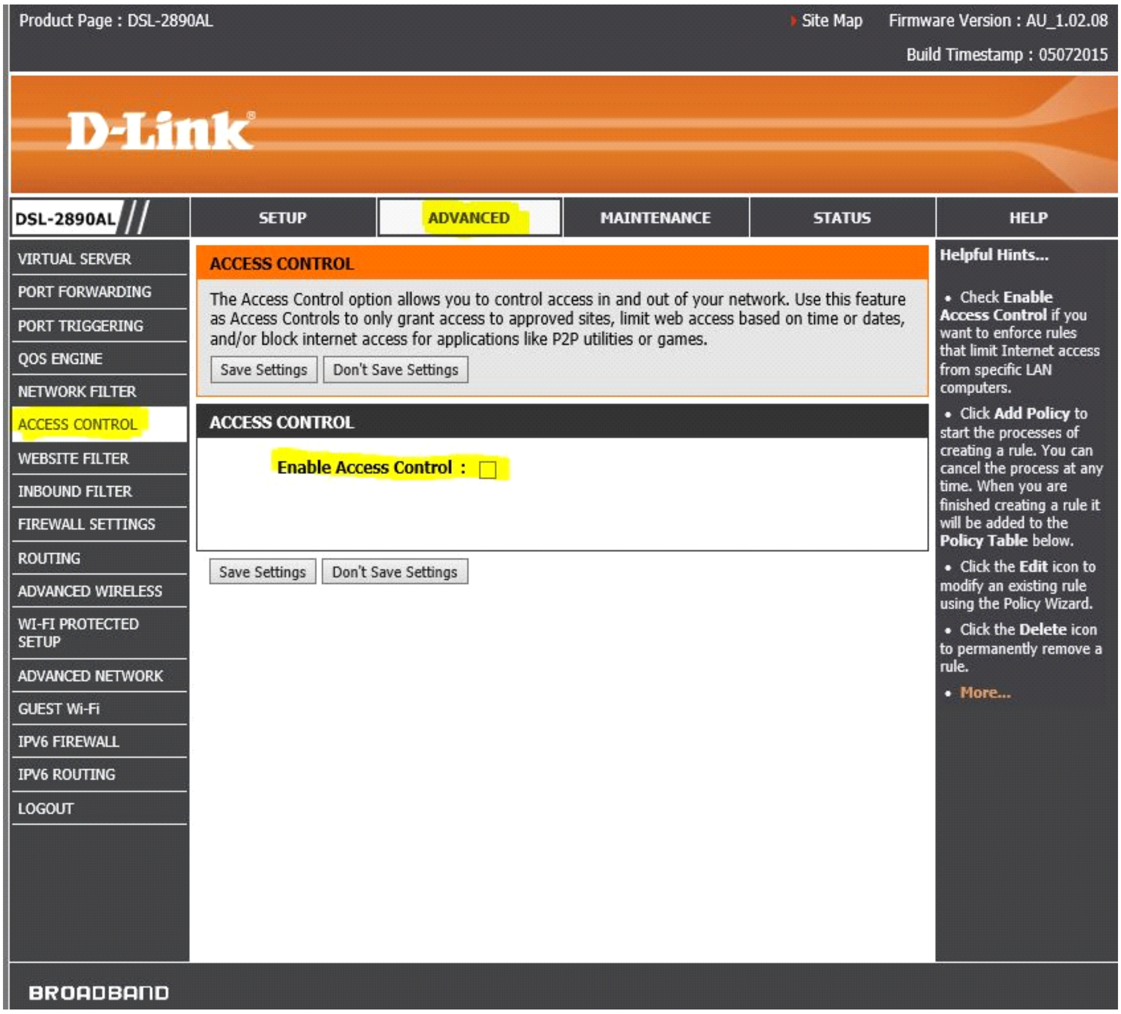
  If you have not changed the password for the modem administration, the factory settings are:

Username: admin

Password: admin

If you cannot recall the password you assigned to your modem you will need to reset the modem to factory defaults by pressing the reset button for 10 seconds. Please note that this will revert all the settings in the modem to factory settings and you will have to reconfigure it with your Internet settings and Wireless security. Make sure you have your Internet account details (given by your Internet Provider) handy.

Step 1. Click on **[ADVANCED]** tab on the top then click on **[ACCESS CONTROL]** menu on the left hand side of the page. Tick the [**Enable Access Control**] option and click on the Save Settings button.



Product Page : DSL-2890AL

Site Map Firmware Version : AU_1.02.08

Build Timestamp : 05072015

ACCESS CONTROL

The Access Control option allows you to control access in and out of your network. Use this feature as Access Controls to only grant access to approved sites, limit web access based on time or dates, and/or block internet access for applications like P2P utilities or games.

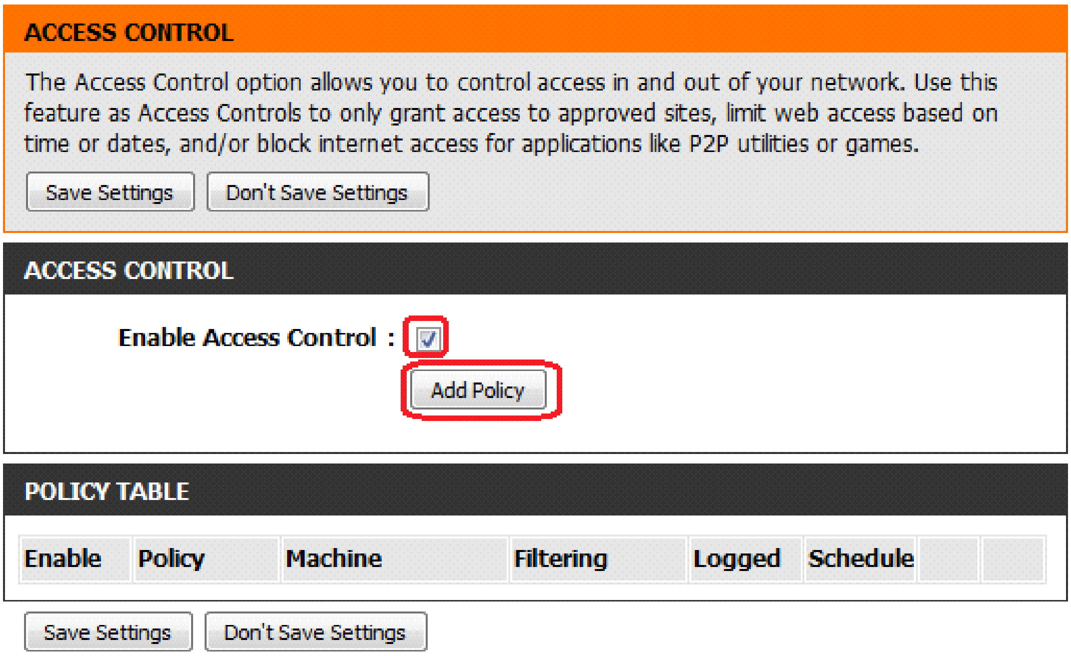
ACCESS CONTROL

Enable Access Control : □

Helpful Hints...

- Check **Enable Access Control** if you want to enforce rules that limit Internet access from specific LAN computers.
- Click **Add Policy** to start the processes of creating a rule. You can cancel the process at any time. When you are finished creating a rule it will be added to the **Policy Table** below.
- Click the **Edit** icon to modify an existing rule using the Policy Wizard.
- Click the **Delete** icon to permanently remove a rule.
- More...

Step 2. Click on [**Add Policy**] button.



ACCESS CONTROL

The Access Control option allows you to control access in and out of your network. Use this feature as Access Controls to only grant access to approved sites, limit web access based on time or dates, and/or block internet access for applications like P2P utilities or games.

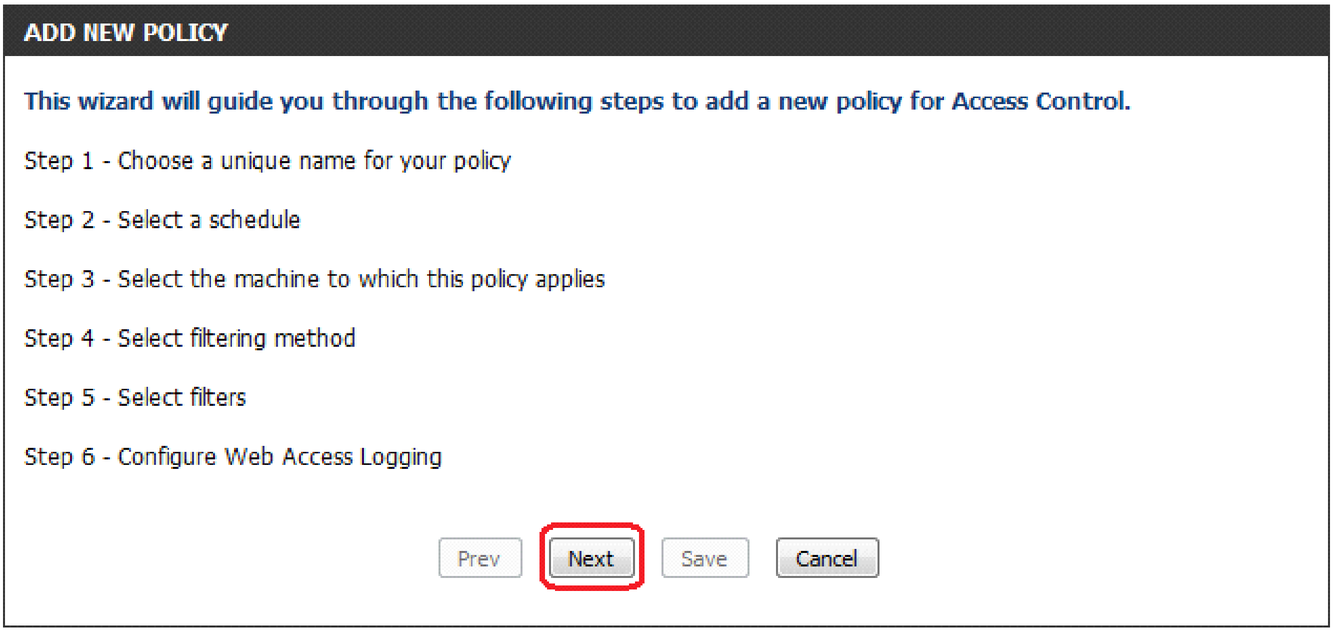
ACCESS CONTROL

Enable Access Control : ☑

POLICY TABLE

Enable	Policy	Machine	Filtering	Logged	Schedule		

Step 3. Go through the Add New Policy Wizard. Click on [**Next**] button to proceed to the next step.



ADD NEW POLICY

This wizard will guide you through the following steps to add a new policy for Access Control.

Step 1 - Choose a unique name for your policy

Step 2 - Select a schedule

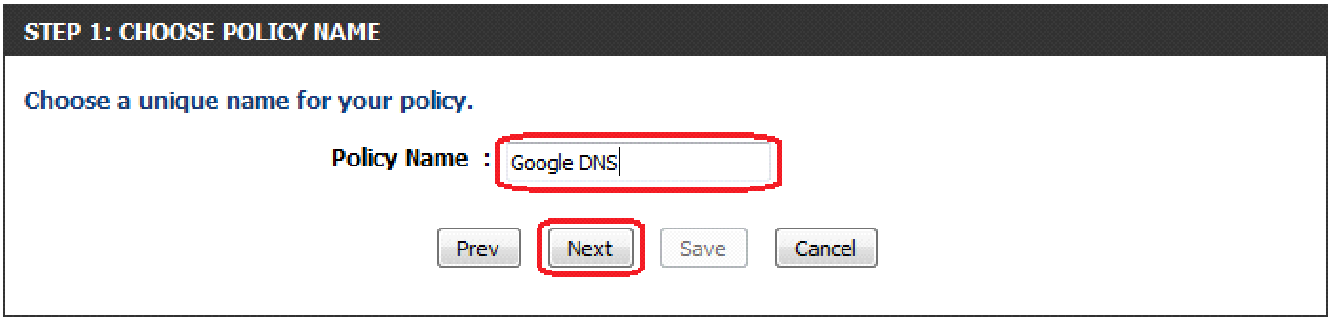
Step 3 - Select the machine to which this policy applies

Step 4 - Select filtering method

Step 5 - Select filters

Step 6 - Configure Web Access Logging

Create a policy name by typing into the section then click on [**Next**] button to proceed.

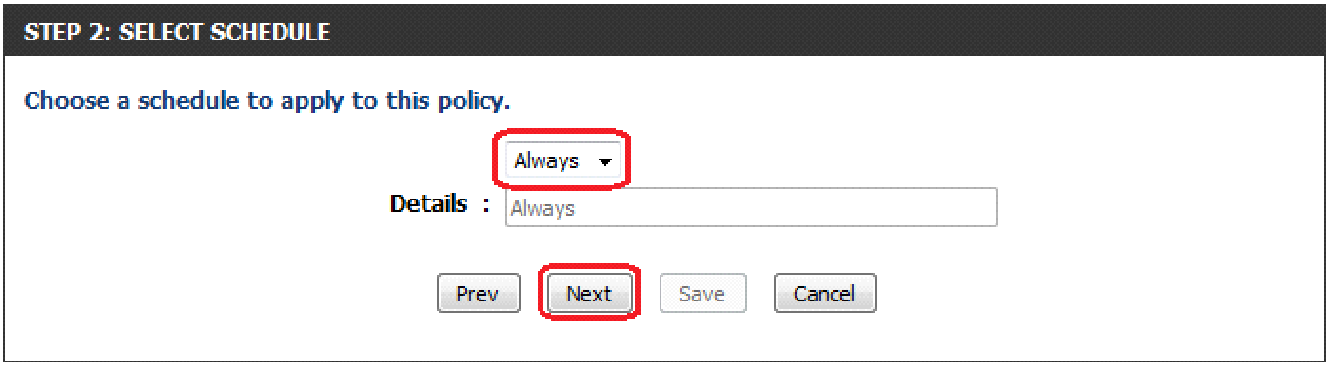


STEP 1: CHOOSE POLICY NAME

Choose a unique name for your policy.

Policy Name : Google DNS

Select [**Always**] if you wish to block Google DNS constantly then click on [**Next**] button to proceed.



STEP 2: SELECT SCHEDULE

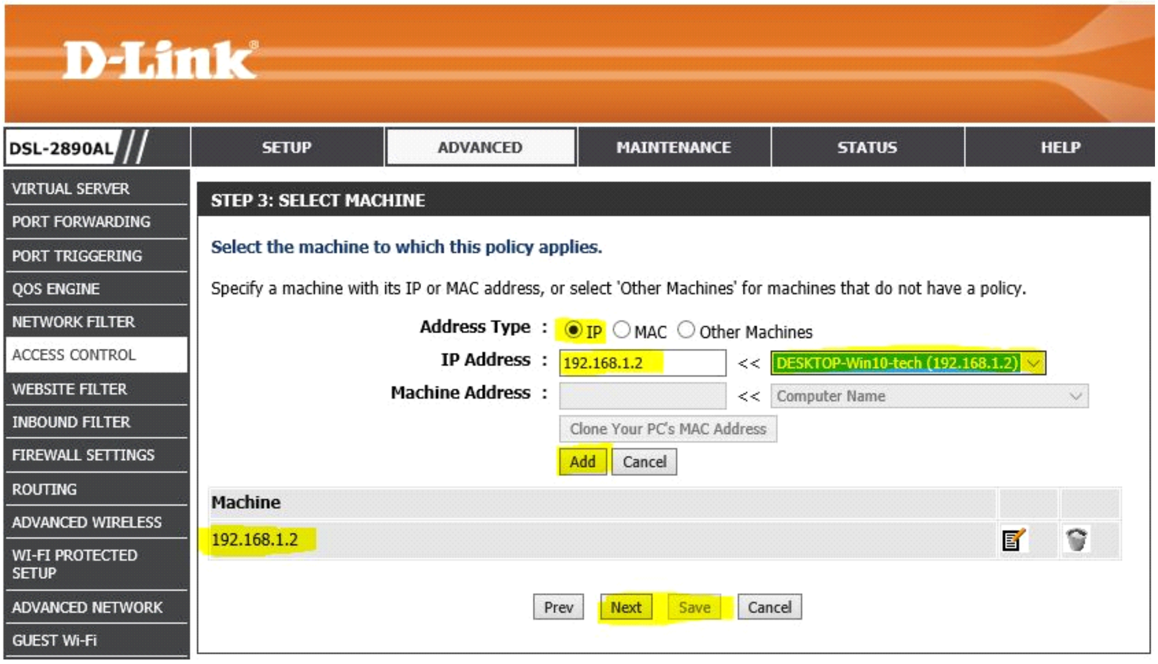
Choose a schedule to apply to this policy.

Always

Details : Always

Choose [**IP Address**] if you wish to apply the policy to a specific IP on the network. Then click on [Add] button to add the option. Click on [**Next**] button to proceed to next step.

You can specify the device(s) by IP address or MAC address or using the Other Machines option.



STEP 3: SELECT MACHINE

Select the machine to which this policy applies.

Specify a machine with its IP or MAC address, or select 'Other Machines' for machines that do not have a policy.

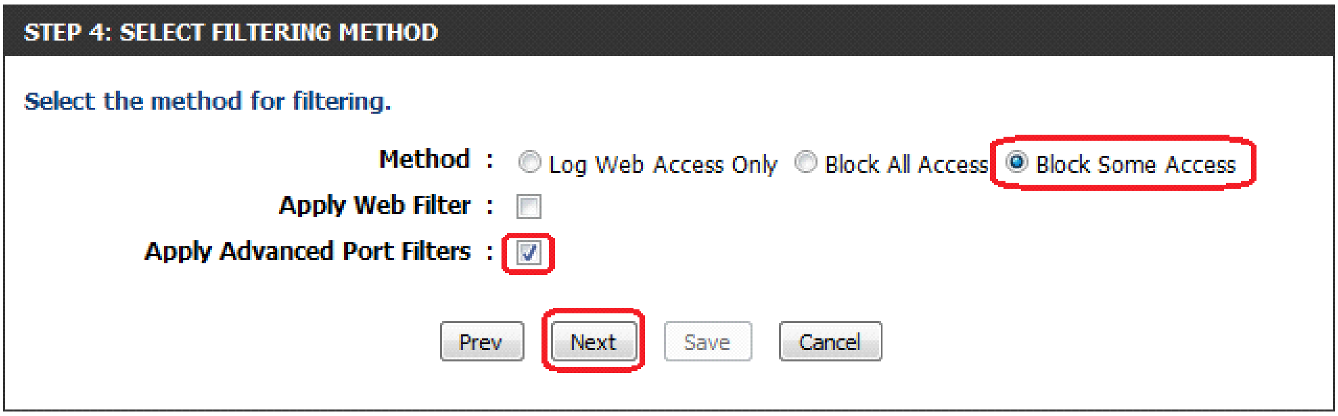
Address Type : ● IP ○ MAC ○ Other Machines

IP Address : 192.168.1.2 << DESKTOP-Win10-tech (192.168.1.2)

Machine Address : << Computer Name

Machine		
192.168.1.2		

Select [**Block Some Access**] and tick the box for [**Apply Advanced Port Filters**] then click on [**Next**] button.



STEP 4: SELECT FILTERING METHOD

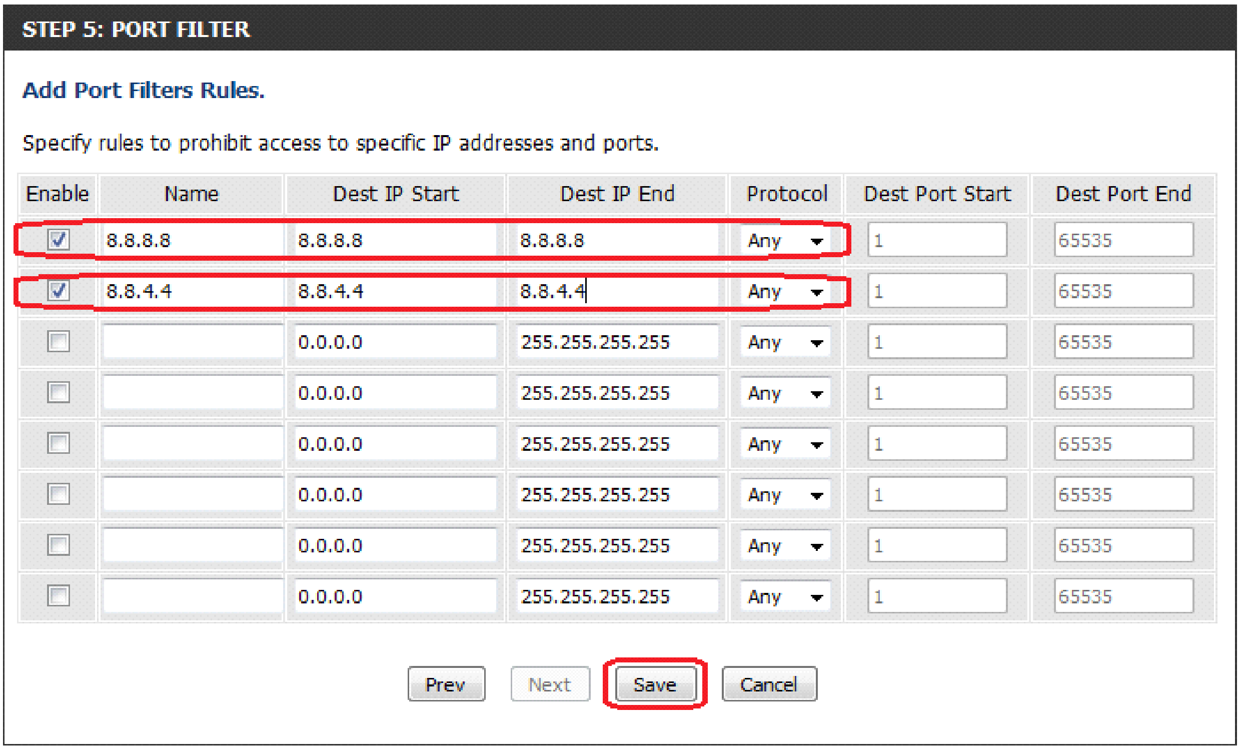
Select the method for filtering.

Method : ○ Log Web Access Only ○ Block All Access ● Block Some Access

Apply Web Filter : □

Apply Advanced Port Filters : ☑

Follow the screenshot below to enter the Internet IP addresses you want to block access to. Make sure the [**Enable**] boxes are ticked then click on [**Next**] button to complete the setup process.



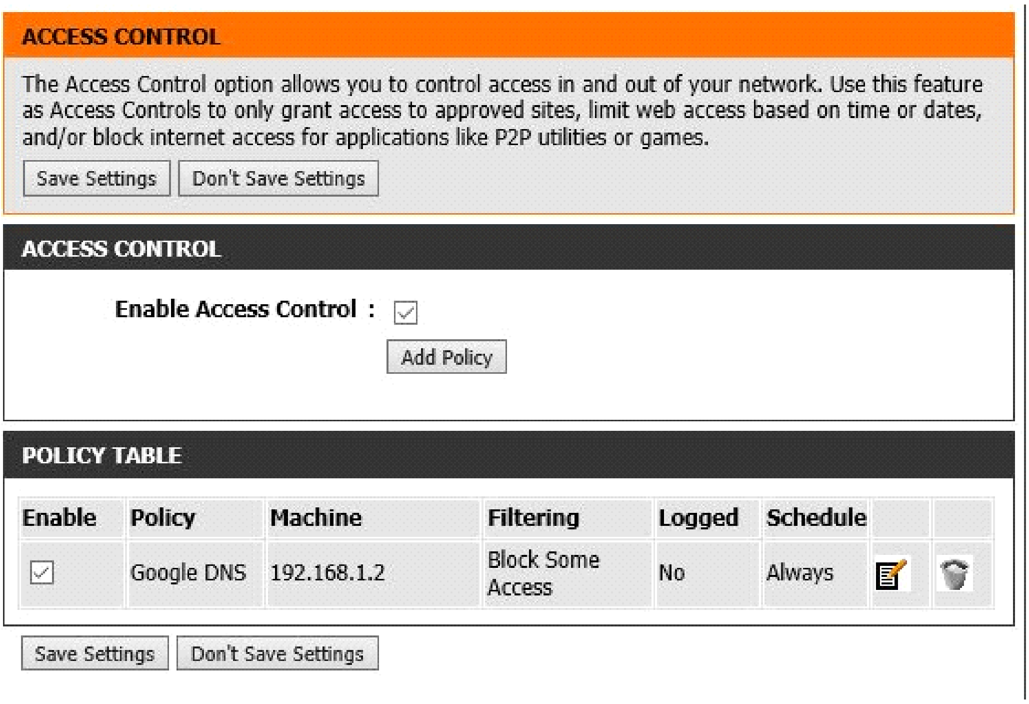
STEP 5: PORT FILTER

Add Port Filters Rules.

Specify rules to prohibit access to specific IP addresses and ports.

Enable	Name	Dest IP Start	Dest IP End	Protocol	Dest Port Start	Dest Port End
☑	8.8.8.8	8.8.8.8	8.8.8.8	Any	1	65535
☑	8.8.4.4	8.8.4.4	8.8.4.4	Any	1	65535
□		0.0.0.0	255.255.255.255	Any	1	65535
□		0.0.0.0	255.255.255.255	Any	1	65535
□		0.0.0.0	255.255.255.255	Any	1	65535
□		0.0.0.0	255.255.255.255	Any	1	65535
□		0.0.0.0	255.255.255.255	Any	1	65535
□		0.0.0.0	255.255.255.255	Any	1	65535

Verify the Policy and ensure the [**Enable**] box is ticked then click on [**Save Settings**] button to apply the settings



ACCESS CONTROL

The Access Control option allows you to control access in and out of your network. Use this feature as Access Controls to only grant access to approved sites, limit web access based on time or dates, and/or block internet access for applications like P2P utilities or games.

ACCESS CONTROL

Enable Access Control : ☑

POLICY TABLE

Enable	Policy	Machine	Filtering	Logged	Schedule		
☑	Google DNS	192.168.1.2	Block Some Access	No	Always		