

# Implementing Access Restrictions for Computers Behind a Linksys VOIP Router

Document ID: 108663

## Contents

### Introduction

How do I implement Access Restrictions for computers behind my router?

### Related Information

## Introduction

This article is one in a series to assist in the setup, troubleshooting, and maintenance of Cisco Small Business products (formerly Linksys Business Series).

Refer to Cisco Technical Tips Conventions for more information on document conventions.

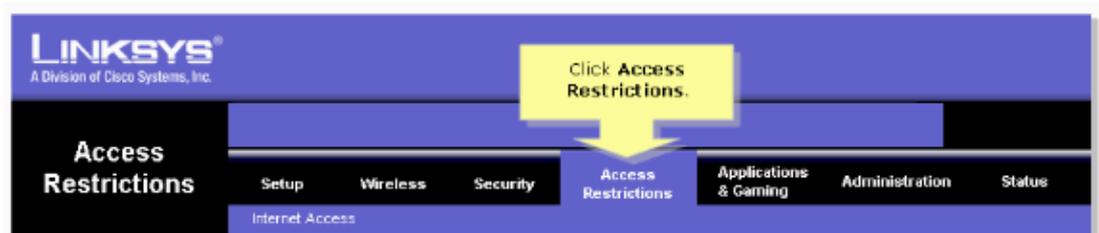
## Q. How do I implement Access Restrictions for computers behind my router?

**A.** Access Restrictions allow you to limit Internet access on your network. You can deny certain computers Internet access, block certain applications, for example, DNS, Ping, HTTP, HTTPS, FTP, POP3, IMAO, SMTP, NNTP, Telnet, SNMP, TFTP and IKE, and services, and block certain websites by the use of keywords or by the URL at a given time. This feature allows you to customize up to ten different Internet Access Policies for particular PCs, which are identified by their IP or MAC Addresses.

### Enable Access Restrictions on a Linksys Router

Complete these steps:

1. Access the web-based setup page of the router. Refer to [Accessing the VOIP Router's Web-Based Setup Page](#) for more information and instructions.
2. When the web-based setup page of the router appears, choose **Access Restrictions > Internet Access**.



3. Choose the policy number from 1 to 10 in the Internet Access Policy drop-down menu.
4. Enter the name of the policy in the Enter Policy Name field such as MyPolicy, and click **Edit List of PCs** in order to add PCs to the policy. A window similar to step 7 appears.

Select the policy number (1-10).

Internet Access Policy : 10 Delete Summary

Status :  Enable  Disable

Enter Policy Name : MyPolicy

PCs : Edit List of PCs

Deny  Allow

Days

Everyday  Wed

Times

24 Hours  From: 12:00 AM To: 12:00 AM

Click **Edit List of PCs** to include computers to the policy.

- When the List of PCs screen appears, specify PCs by IP Address or MAC Address. Enter the appropriate IP Addresses into the IP fields. If you have a range of IP Addresses to filter, complete the appropriate IP Range fields. Enter the appropriate MAC Addresses into the MAC fields.

### List of PCs

Enter MAC Address of the PCs in this format : xxxxxxxxxx

MAC 01 : 00:00:00:00:00:00 MAC 05 : 00:00:00:00:00:00

MAC 02 : 00:00:00:00:00:00 MAC 06 : 00:00:00:00:00:00

MAC 03 : 00:00:00:00:00:00 MAC 07 : 00:00:00:00:00:00

MAC 04 : 00:00:00:00:00:00 MAC 08 : 00:00:00:00:00:00

Enter the IP Address of the PCs

IP 01 : 192.168.1. 0 IP 04 : 192.168.1. 0

IP 02 : 192.168.1. 0 IP 05 : 192.168.1. 0

IP 03 : 192.168.1. 0 IP 06 : 192.168.1. 0

Enter the IP Range of the PCs

IP Range 01 : 192.168.1. 0 ~ 0

IP Range 02 : 192.168.1. 0 ~ 0

Either enter the computer's **MAC Address** here.

And/or enter the computer's **IP Address** here.

And/or enter the computer's **IP Range** here.

**Note:** The reason Linksys provides three columns (MAC Address, IP Address and IP Range) is to let you key-in based on the address. For example, if a customer has MAC Addresses to be restricted, then you need to key-in the particular MAC Addresses in the MAC Address column; it is the same for IP Address. For IP Range, if you want to restrict a group of IP Addresses, for example 192.168.1.20 to 192.168.1.40, then you need to key-in the range of IP Addresses in IP Range column.

6. Click **Save Settings**, and then close the window in order to return to the Internet Access screen.
7. If you want to block the listed PCs from Internet access during the designated days and time, choose **Deny**.
8. Set the days when access is filtered. Choose **Everyday** or the appropriate day/s of the week.
9. Set the time when access is filtered. Choose **24 Hours** or choose the box next to **From** and choose a specific time period from the drop-down boxes.

The screenshot shows the 'Internet Access' configuration window. At the top, there is a header 'Internet Access' and a dropdown menu for 'Internet Access Policy' set to '10', with 'Delete' and 'Summary' buttons. Below this, the 'Status' is set to 'Enable'. The 'Enter Policy Name' field contains 'MyPolicy'. Under 'PCs', there is an 'Edit List of PCs' button. The 'Internet access during selected days and hours' section has three sub-sections: 'Days', 'Times', and 'Status'. In the 'Days' section, 'Everyday' is checked. In the 'Times' section, '24 Hours' is selected. In the 'Status' section, 'Deny' is selected. Three yellow callout boxes with arrows point to these specific settings: 'Select Deny.', 'Select Everyday or the appropriate days of the week.', and 'Select 24 Hours or check the box next to From and select a specific time period from the drop-down boxes.'

10. Click **Save Settings**.
11. Repeat steps 3–10 in order to create or edit additional policies.

## Related Information

- [Technical Support & Documentation – Cisco Systems](#)

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2013 – 2014 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Dec 12, 2008

Document ID: 108663