Home Network Manager User Guide

version 2.4

Mediacom

100 Crystal Run Road
Middletown, NY 10091
+1 855 558 5812
www.mediacomcable.com

February 2011

Table of Contents

Home Network Manager Overview

The Mediacom Home Network Manager is a browser-based application that helps you manage, protect and share your home network. It enables you to easily modify basic home network configuration such as wireless, firewall, and port forwarding, and provides a way to setup enhanced services such as time blocking and content filtering. The HMN provides remote access to the home network, providing a one-click process to access any IP-enabled device in the home.

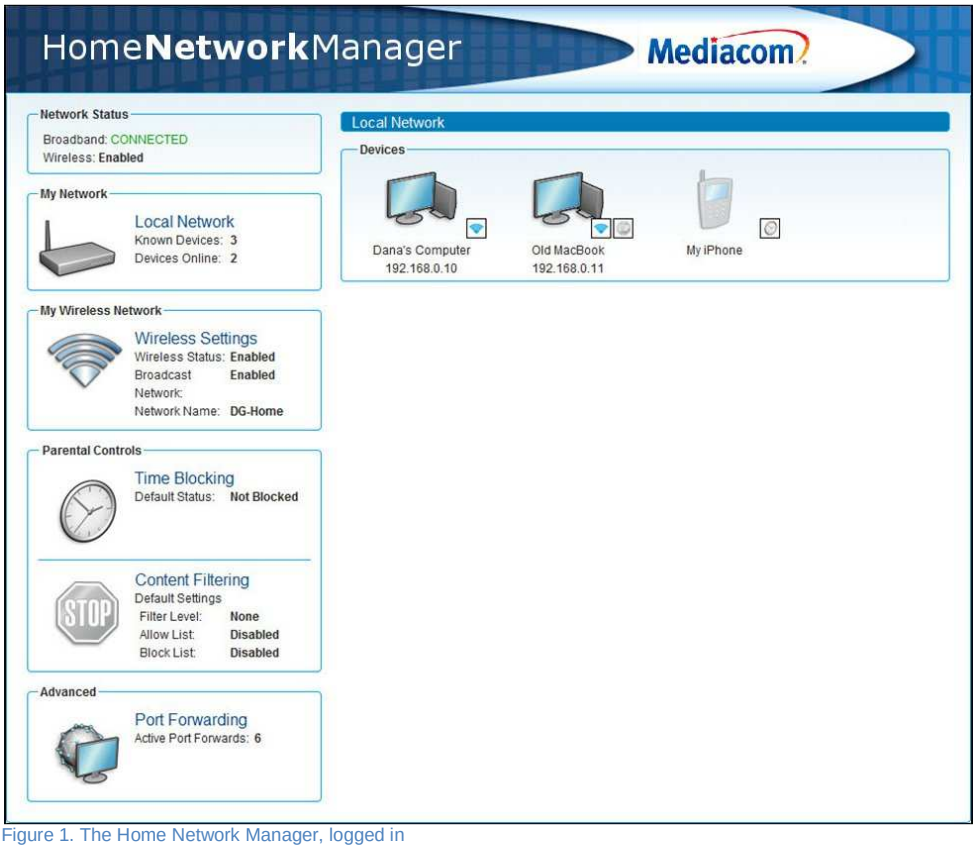


Figure 1. The Home Network Manager, logged in

Network Status

Shows whether your broadband is connected, and whether wireless networking is enabled.

My Network

This shows how many LAN devices are known to your local network, and how many are online. When you log in, the complete list of devices connected to your network is automatically displayed on the right-hand side of the screen.

My Wireless Network

This is the location where you can manage your wireless network settings. You can enable or disable your wireless, or modify your wireless settings, such as changing your WEP Key, changing the wireless broadcast channel, and enabling/disabling the broadcast of your SSID.

Parental Controls

This is the location where internet access controls are managed. A summary of the current service settings is displayed. Clicking on each service link will bring up a window where you can view and edit settings for that service.

- **Content filtering**: Content filtering is used to prevent users from viewing inappropriate web sites or content. Filtering can be implemented on individual computers and devices or on the entire network. It is possible for different computers and devices on the network to have different levels of internet access. There are two types of content filtering: Basic content filtering and Dynamic content filtering.
    - Basic content filtering uses lists of Allowed web sites [whitelist] and Blocked web sites [blacklist].
    - Dynamic content filtering allows you to select an age-group filtering level – this service checks each web site against a master list maintained by your service provider. The master list checks site content and blocks sites inappropriate to the age-group indicated by the filter level.
- **Time blocking**: The time blocking application in the Home Network Manager allows you to set limits on how much time the internet can be accessed. You can set individual blocks of time throughout the week to be blocked, limit the amount of time the internet can be accessed each day, and limit the amount of time it can be accessed each week. You can also use the Bonus Time feature to override the normal schedule and add timed access starting immediately for a set amount of time.

Advanced

This is the location where you can manage port forwards. This powerful feature of the Home Network Manager gives you the ability to remotely configure port forward settings for specific LAN devices. Port forwarding is usually necessary to play online games or deploy VoIP services behind an enabled gateway.

My Network

The Local Network page provides summary information about individual devices that are connected to your local network.

Figure 2: Default view of the Local Network summary in the My Network area

For each device, the name, icon, IP address, and connection status is shown. Also, small icons show if any services such as content filtering or time blocking have been applied to the device.

Figure 3: View of the Local Network pane in the My Network area, showing information for a specific device.

Hovering over a device with your mouse cursor will display a small window providing more information about applied services. Clicking on the device icon or name will load the Device Detail page for that device.

Device Detail

The Device Detail page provides summary information about an individual device that is connected to your local network. You can find information on the manufacturer, MAC address, and current IP address; view the currently active services; and configure access to a local management interface, if the device supports such management.

Figure 4: Device Detail summary page

When viewing the detail for a specific device, you can change back to viewing the summary of all of your local network devices by clicking on the “Devices” breadcrumb immediately below the “Local Network” header.

On the Device Detail page, you can change the name of the device as it is listed on the network. You can also assign an icon from the available ones to best match the device, such as an iPad, a laptop, or a desktop computer. The Device Detail page also allows you to view and edit the active services for the device.

Task: I want to change the name of a device on the network, and select a different icon

1. Login to the Home Network Manager.
2. In the Devices section, click the link to the device you want to edit. This opens the Device Details page for that device.
3. In the Device Information section, click the Edit Name and Icon button.

4. This brings up the Edit Device Name and Icon window, where you can select which icon you’d like and edit the device name.

5. Type in the new name for the device, and if desired select an icon to represent it.
6. Click the OK button.
7. Click the Save button. You must click the Save button to save the changes to your gateway, or changes will be lost when you navigate away from the page.
8. Logout from the Home Network Manager.

Task: I want to access the local management interface for a manageable device

Some devices, such as webcams, may have a local management interface that you can access as a web page. This management interface might allow you to schedule events or view camera pictures. If your device has a local management interface, the manual will tell you how to access it directly from your web browser. The Home Network Manager also allows you to configure a link to the local management interface within the Home Network Manager, so you do not need to remember the URL.

Enabling access to the local interface for a device from within the Home Network Manager also allows you to access the interface from computers that are not on your local network. For example, this would allow you to view the webcam images from your office computer. Note that this could be a potential security risk, so remember to disable this function when you're not using it.

1. Login to the Home Network Manager.
2. In the Devices section, click the link to the device you want to edit. This opens the Device Details page for that device.
3. In the View Local Interface section, click the Enable Local Interface Access button.
4. In the dialog box, enter the port number for access, if your user's manual specifies a port. This will allow access only to that specific port. If your user's manual does not specify a port, it will default to port 80.
5. Enter the path for the location to be accessed, if your user's manual specifies one. This will allow access only to that specific path.
6. Click the OK button.
7. Click the Save button. You must click the Save button in order to save the changes to your gateway, or changes will be lost when you navigate away from the page.
8. Logout from the Home Network Manager.

Task: I want to delete a device from the network

1. Login to the Home Network Manager.
2. In the Devices section, click the link to the device you want to delete. This opens the Device Details page for that device.
3. In the Device Information section, click the Delete Device button. This will delete the device from the list of devices on the network. Note that if that device connects to your network at a later time, it will reappear and the previous settings will be applied.

4. Click the OK button.
5. Click the Save button. You must click the Save button in order to save the changes to your gateway, or changes will be lost when you navigate away from the page.
6. Logout from the Home Network Manager.

Wireless Service

You can enable or disable your wireless, or modify your wireless settings, such as changing your WEP Key, changing the wireless broadcast channel, and enabling/disabling the broadcast of your SSID.

Figure 5: Default view of the wireless summary in the Basic Services area

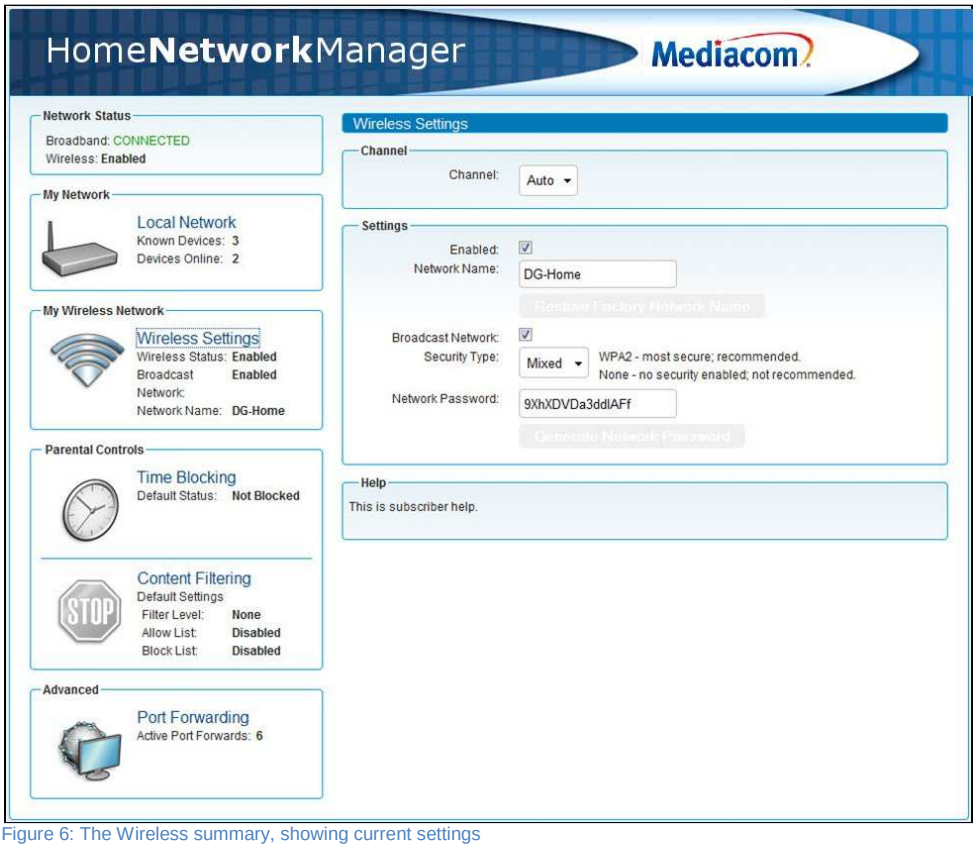


Figure 6: The Wireless summary, showing current settings

Task: I want to turn on wireless networking

When you first receive the wireless modem, wireless may not be turned on/enabled. This shows you how to turn on wireless service and describes other options you should consider when setting up wireless networking.

1. Login into the Home Network Manager.
2. Click on the Wireless Settings link under Basic Services. This opens the Wireless summary pane on the right side of the screen.
3. Enter your SSID in the text box, or leave the default name. This is a name for the wireless network that allows your wireless network to be identified.
4. Use the drop-down arrow next to Security Type to choose the security type and enter the key if applicable. WPA2 is recommended.
5. Click the Enabled check box. When checked, wireless networking will be enabled after saving the configuration in a later step.
6. (Optional) If you want to broadcast the availability of your wireless network, click the check box next to Broadcast.
    - NOTE: If you broadcast the beacon, the Network Name (SSID) and the security status icon will be displayed to computers within reach. If you do not set up a Security Type with a security key, your network will be open and available to any computer that can see the beacon. To set up a security key, follow the steps in the next section under “I’d like my wireless to be secure.”
7. Click the OK button.
8. Click the Save button. You must click the Save button in order to save the changes to your gateway, or changes will be lost when you navigate away from the page.
9. Logout from the Home Network Manager.

Task: I’d like my wireless to be secure

When you enable wireless service on your wireless modem, you can also set up your security options.

1. Login into the Home Network Manager.
2. Click on the Wireless link under Basic Services. This opens the Wireless summary pane on the right side of the screen.
3. Click the Enabled check box. When checked, wireless networking will be enabled after saving the configuration in a later step.
4. Click the Broadcast check box. When checked, your Network Name (SSID) and security status will be broadcast to any computer within reach.
5. Type in the network name that you’d like to use in the Network Name (SSID) field. For example, you can use a name and the word network, such as “Jack’s Network.”
    - NOTE: Pick something meaningful to you, to make it easier for you and any visitors to select and log into the correct network.

6. To change the channel on which the radio broadcasts its signal, please choose a channel number from 1 to 11 by clicking the drop-down arrow. The default Security Channel value is Auto.
    - NOTE: This functionality is useful if the gateway's radio is interfering with other wireless devices in your environment or vice versa (other wireless devices affecting the gateway's ability to transmit wireless signals properly). Unless there are other wireless devices using the same channel, the security channel should be set to Auto.
7. Use the arrows to select a Security Type. If you select anything other than None or Mixed, you'll need to use the automatically generated security key or create your own. The types are listed below, in order of most secure to least secure.
    - WPA2
    - WPA
    - WEP
    - Mixed
    - None
8. Click the Generate Wireless Key button, unless you are using your own custom security key. If using your own custom security key, type the key into the text box.

    NOTE: Dictionary words should not be used for custom security keys. A random generation of letters and numbers makes for a stronger security key.
9. Click the OK button.
10. Click the Save button. You must click the Save button in order to save the changes to your gateway, or changes will be lost when you navigate away from the page.
11. Logout from the Home Network Manager.

Task: I'd like to allow someone visiting to log into my wireless network

When you have a guest visit your home, if the wireless network is already enabled you simply need to tell your guest the SSID and security key. If you do not already have the wireless network enabled, follow the instructions under "I want to turn on wireless networking" and then give your guest the SSID and security key.

Time Blocking

The time blocking application in the Home Network Manager allows you to set time blocking rules. Customers can set individual blocks of time throughout the week to be blocked, limit the amount of time the internet can be accessed each day, and use the Bonus Time feature to override the normal schedule and add timed access starting immediately for a set amount of time.

Figure 7: Default view of the time blocking application in the Basic Services area

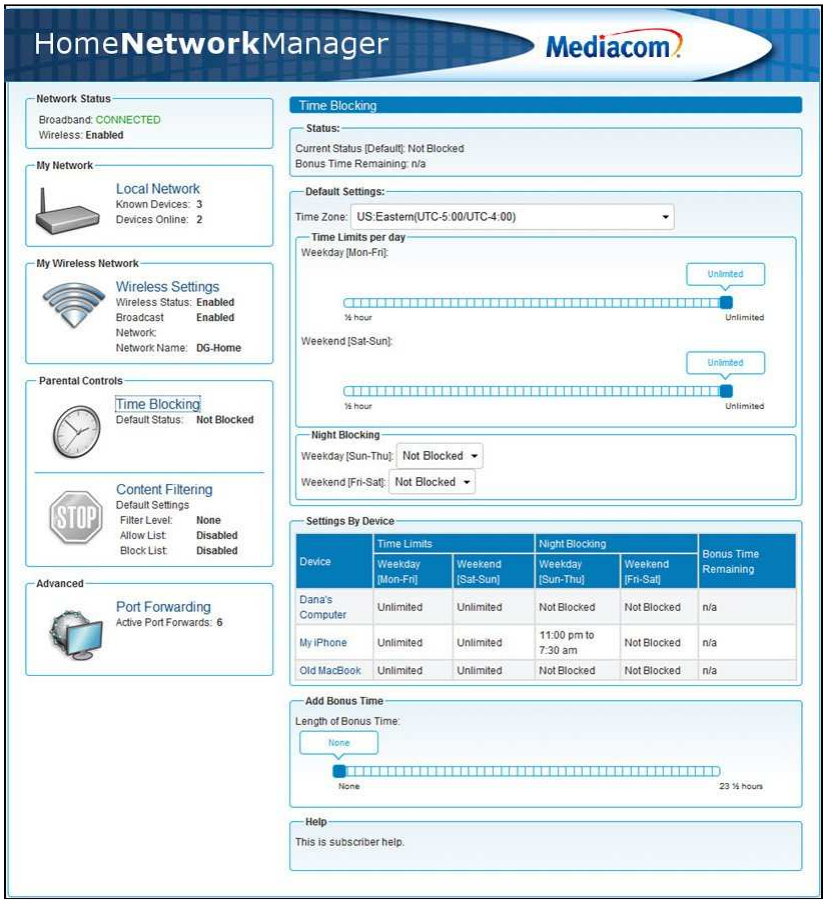


Figure 8: The Time Blocking detail, showing current settings

Task: I want to block all computers in the house from Internet access during certain hours

Use this feature when you want to block anyone in the house from accessing the Internet during certain hours. For example, you can block after bedtime hours on weekdays and have a different time blocked on weekend nights. Note that when you set or change the default settings, these changes apply only to devices that first connect to the router after the default settings have been changed. To change settings for a device that is already listed in the device list, you need to configure that device manually.

1. Login into the Home Network Manager.
2. Click on the Time Blocking link under Basic Services. This opens the Time Blocking summary pane on the right side of the screen.
3. In the Default Settings section, under Night Blocking, click on the arrows next to Weekday to select the times during the week when you want to block all computers from accessing the Internet. Weekday nights are Sunday, Monday, Tuesday, Wednesday, and Thursday nights.
4. Click the arrows next to Weekend to select the times on weekends you want to block all computers from accessing the Internet. Weekend nights are Friday and Saturday nights.

   Note: Time can be blocked in half hour increments.
5. Click the OK button.
6. Click the Save button. You must click the Save button in order to save the changes to your gateway, or changes will be lost when you navigate away from the page.
7. Logout from the Home Network Manager.

Task: I want to block a device from accessing the Internet during certain hours

Use this feature when you want to make sure that devices are not connecting to the Internet during certain hours. This means features like Xbox Live or web surfing will not work, although games with local single player options will still be able to run.

1. Login into the Home Network Manager.
2. Click on the Time Blocking link under Basic Services. This opens the Time Blocking summary pane on the right side of the screen.
3. Click on the device in the Settings by Device section.
4. In the Night Blocking section, select Blocked and then use the arrows to select the start and stop times for blocking access. This will limit Internet access for this device only during the time period specified on weekday nights. Weekday nights are Sunday, Monday, Tuesday, Wednesday, and Thursday nights.
   - Example: If you set the times to 10 pm to 6 am, a person using this device cannot access the Internet using this device during those hours each day on Monday through Friday.
5. In the Night Blocking section, select Blocked and then use the arrows to select the start and stop times for blocking access. This will limit Internet access for this device only

during the time period on weekend nights. Weekend nights are Friday and Saturday nights.

- Example: If you set the times limit to 10 pm to 6 am, a person using this device cannot access the Internet using this device during those hours each day on Saturday and Sunday.

6. Click the OK button.
7. Click the Save button. You must click the Save button in order to save the changes to your gateway, or changes will be lost when you navigate away from the page.
8. Logout from the Home Network Manager.

Task: I want to limit the amount of time a device can connect to the Internet

1. Login into the Home Network Manager.
2. Click on the Time Blocking link under Basic Services. This opens the Time Blocking summary pane on the right side of the screen.
3. Click on the device in the Settings by Device section.
4. In the Time Limits per day section, click and drag the Weekday slider to select the number of hours allowed. You can limit time in 30 minute time blocks. This will limit Internet access for this device only to the number of hours specified on Monday through Friday.
    - Example: If you set the time limit at 4 hours, a person using this device can only access this device for a total of 4 hours each day on Monday through Friday.
5. In the Time Limits by day section, click and drag the Weekend slider to select the number of hours allowed. You can limit time in 30 minute time blocks. This will limit Internet access for this device only to the time period on Saturday and Sunday.
    - Example: If you set the time limit at 4 hours, a person using this device can only access the internet using this device for a total of 4 hours each day on Saturday and Sunday.
6. Click the OK button.
7. Click the Save button. You must click the Save button in order to save the changes to your gateway, or changes will be lost when you navigate away from the page.
8. Logout from the Home Network Manager.

Task: I want to give some extra time on a device just for today without changing my normal time blocking settings

If you want to give some extra time on the Internet for a device, but don't want to change your normal time blocking settings, you can use this procedure. This will temporarily override the time blocking settings on this device.

1. Login into the Home Network Manager.

2. Click on the Time Blocking link under Basic Services. This opens the Time Blocking summary pane on the right side of the screen.
3. In the Settings by Device section, click on the device for which you want to add bonus time. This opens the Edit Time Blocking window for that device.
4. Click and drag the slider under Add Bonus Time. You can give time in 30 minute time blocks. This bonus time takes effect immediately, once saved as shown in step 6.
    - Example: It's 4 p.m., you want to give an Xbox gaming device access to the Internet until midnight, and time blocking normally starts at 7 p.m., you can set bonus time for 8 hours. This will override the 7 p.m. start for today only, and will not change the settings permanently.
5. Click the OK button.
6. Click the Save button. You must click the Save button in order to save the changes to your gateway, or changes will be lost when you navigate away from the page.
7. Logout from the Home Network Manager.

Task: I want to give some extra time for all devices on the network just for today without changing my normal time blocking settings

If you want to give some extra time on the Internet for a device, but don't want to change your normal time blocking settings, you can use this procedure. This will temporarily override the time blocking settings on this device.

1. Login into the Home Network Manager.
2. Click on the Time Blocking link under Basic Services. This opens the Time Blocking summary pane on the right side of the screen.
3. Click and drag the slider under Add Bonus Time. You can give time in 30 minute time blocks. This bonus time takes effect immediately, once saved as shown in step 5.
    - Example: It's 4 p.m., you want to give network access to the Internet until midnight, and time blocking normally starts at 7 p.m., you can set bonus time for 8 hours. This will override the 7 p.m. start for today only, and will not change the settings permanently.
4. Click the OK button.
5. Click the Save button. You must click the Save button in order to save the changes to your gateway, or changes will be lost when you navigate away from the page.
6. Logout from the Home Network Manager.

Task: I want to see the time blocking settings on my entire network

If you are not sure what settings are on each device in your network, you can see a summary of current time blocking settings using the following procedure:

1. Login into the Home Network Manager.
2. Click on the Time Blocking link under Basic Services.
3. The Time Blocking information for the network is in the Time Blocking pane on the right of your screen.

4. Logout from the Home Network Manager.

Task: I want to see the time blocking settings for a particular device

If you are not sure what settings are on for a specific device in your network, you can see the current time blocking settings using the following procedure:

1. Login into the Home Network Manager.
2. Click on the Time Blocking link under Basic Services. This opens the Time Blocking summary pane on the right side of the screen.
3. The Time Blocking information for the device is in the Settings by Device section.
4. If you want to change the settings for that device, in the Settings by Device section, click on the link for the device to edit those settings. Follow the instructions in the section above on how to apply time blocking for a particular device on the network.
5. If you have made changes, click the OK button and then click the Save button. You must click the Save button in order to save the changes to your gateway, or changes will be lost when you navigate away from the page.
6. Logout from the Home Network Manger.

Content Filtering

Content filtering is used to prevent users from viewing inappropriate web sites or content. Filtering is implemented on individual computers and devices or on the entire network. It is possible for different computers and devices to have different levels of internet access.

Figure 9: Default view of the content filtering summary in the Basic Services area

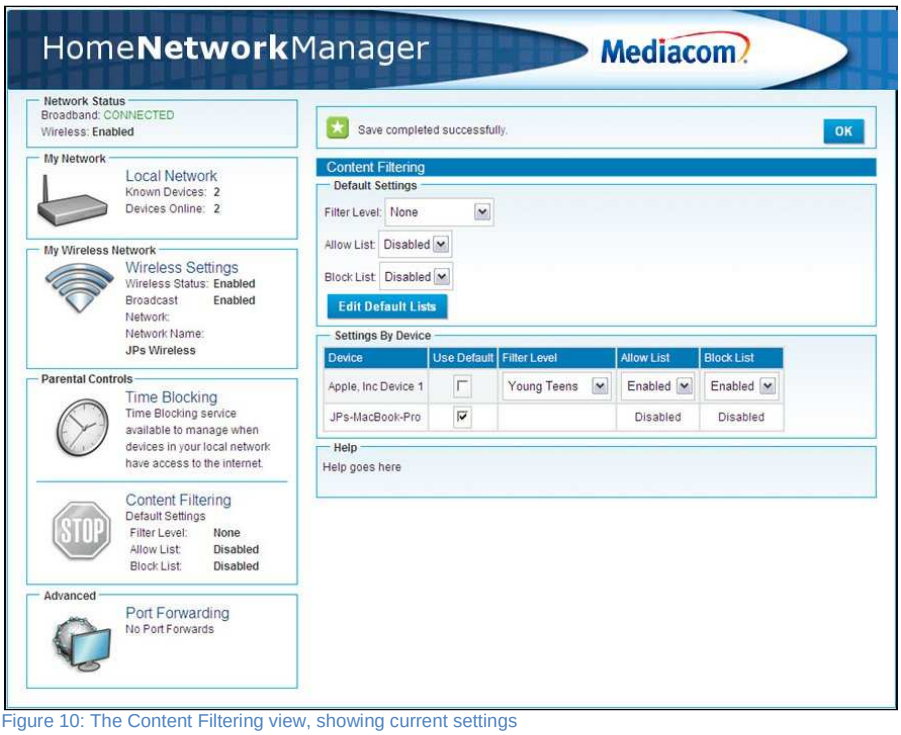


Figure 10: The Content Filtering view, showing current settings

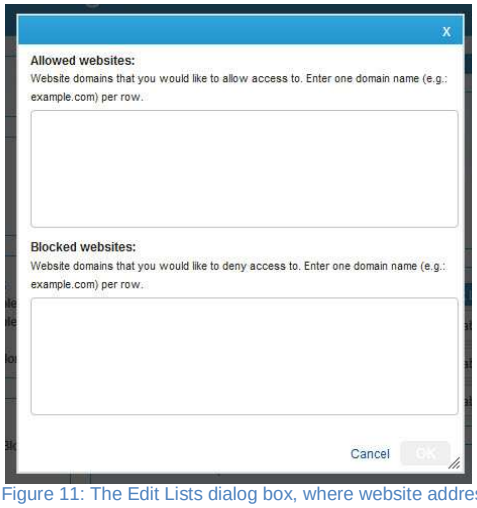


Figure 11: The Edit Lists dialog box, where website addresses are entered for allowed or blocked websites

You can choose from several filter levels:

6 and Under. The 6 and Under filter level is different from the other filter levels in that it allows access only to certain sites rather than blocking some categories of sites and allowing all others. The 6 and Under filter allows access only to sites categorized as appropriate for children. All other addresses are blocked. If you want to allow access to additional sites, the site addresses must be added to the Allow list.

Ages 7 - 12. The Ages 7 - 12 filter blocks a wide range of content categorized as inappropriate for young children as well as web-based communications, including access to webmail systems, chatting and chat sites, and forums and message boards. File sharing is not allowed. Sites that are not categorized as inappropriate are allowed. You can block additional content by adding specific addresses to the Block list or allow blocked content by adding addresses to the Allow list.

Ages 13 - 16. The Ages 13 - 16 filter blocks content categorized as inappropriate for young teens. It also blocks file sharing, chatting and chat sites, dating sites, and virtual communities. It does allow access to webmail and blogging. Sites that are not categorized as inappropriate are allowed. You can block additional content by adding specific addresses to the Block list or allow blocked content by adding addresses to the Allow list.

Ages 17 -18. The Ages 17 -18 filter blocks sites categorized as pornography, alcohol, anonymizers, drugs, gambling hate, tobacco, violence, and weapons. There are no restrictions on file sharing, webmail or chat, or virtual communities. Sites that are not categorized as inappropriate are allowed. You can block additional content by adding specific addresses to the Block list or allow blocked content by adding addresses to the Allow list.

You can also use the Allow and Block lists to fine-tune the sites devices are able to access. Here are some things to know about how the lists work and how they interact with filter levels.

- Only one Allow list and one Block list can be used. You can enable or disable the lists for each device on the network, but all devices use the same Allow and Block lists.
- If you have the Allow list enabled, but do NOT have a filter level set, the device can access only addresses on the Allow list.

For example, imagine you have a child's computer for which an Allow list is enabled. The Allow list contains *disney.com* and *nickelodeon.com*. No filter level is applied. This computer can access only two sites: *disney.com* and *nickelodeon.com.*

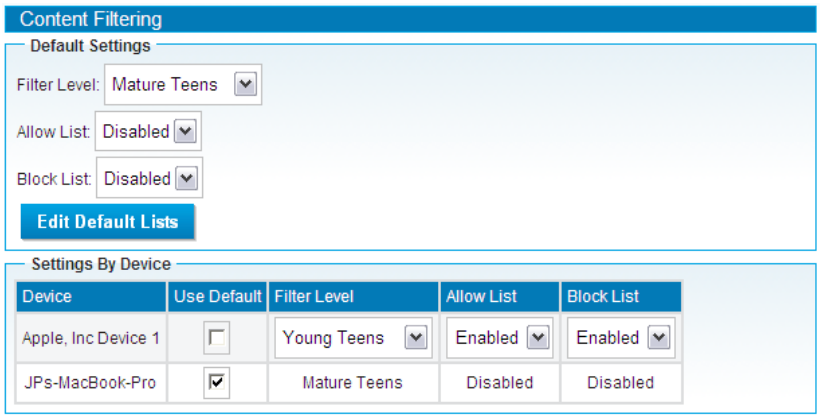
- If you have a filter level set, you can override its settings by adding addresses to the Allow and Block lists.

For example, imagine you have a computer that your 15-year-old uses. You have applied an Age 13 - 16 filter to this computer. You have also enabled the Allow and Block lists. The Block list contains *YouTube.com*. The Allow list contains bigbeer.com. Although the Age 13 -16 filter would normally allow *YouTube.com* and block *bigbeer.com*, this computer cannot access *YouTube.com*, but can access *bigbeer.com*.

Task: I want to restrict access by age level

You can use the Filter Level settings to block access to categories of sites by age level. (Note that the filter categories available to you may have different names.)

2. Log in to the Home Network Manager.
3. Click the Content Filtering link under Basic Services to open the Content Filtering summary pane on the right side of the screen.
4. In the Default Settings area, choose a default filter level from the Filter Level menu. This becomes the default for your network. Any new devices joining the network use this level.



5. In the Settings By Device area, choose a filter level for each device or select the Use Default check box to use the default filter level.
6. Click the Save button. You must click the Save button in order to save the changes to your gateway, or changes will be lost when you navigate away from the page.
7. Log out of the Control Panel.

Task: I don't want anyone on the network to go to this website

If there are certain websites you do not want devices to have access to, you can explicitly block just those websites for the entire network, using content filtering.

1. Log in to the Home Network Manager.
2. Click on the Content Filtering link under Basic Services. This opens the Content Filtering summary pane on the right side of the screen.
3. In the table in the Default Settings area, click the Edit Default Lists button. This opens a window where you can enter allowed or blocked website addresses.

4. Type in each website address you want blocked, one address per row/line.
    - Use the following format for each website address: www.websitename.xxx (where .xxx is .com, .net, .biz, etc.).
    - Do not use http:// or https:// before website addresses.
    - If you are blocking a site such as Yahoo or Google, be very careful in how you type the address.
        - www.yahoo.com will block the front page of Yahoo.com, but will not block other services such as Yahoo Messenger (messenger.yahoo.com) or Yahoo Mail (mail.yahoo.com).
        - Entering yahoo.com will block all services from Yahoo.com, including Mail, Messenger, and Flickr.
5. Click the OK button.
6. Click the Save button. You must click the Save button in order to save the changes to your gateway, or changes will be lost when you navigate away from the page.
7. Log out of the Home Network Manager.

Note that you can enable the Block list for a specific device instead of the whole network.

Task: I want to restrict access to a specific list of sites

You can set up an Allow list to allow access to specific sites while blocking all others. (Note that the Allow list can also be used to override filter levels. See the following task for more information.)

1. Log in to the Home Network Manager.
2. Click the Content Filtering link under Basic Services. This opens the Content Filtering summary pane on the right side of the screen.
3. In the table in the Default Settings area, click the Edit Default Lists button. This opens a window where you can enter allowed or blocked website addresses.
4. Type in each website address you want to allow, one address per row/line.
    - Use the following format for each website address: www.websitename.xxx (where .xxx is .com, .net, .biz, etcetera).
    - You cannot use http:// or https:// before website addresses.
    - If you are allowing a site such as Yahoo or Google, be very careful in how you type the address.
        - www.yahoo.com will allow the front page of Yahoo.com, but will not allow other services such as Yahoo Messenger (messenger.yahoo.com) or Yahoo Mail (mail.yahoo.com).
5. Click OK.
6. In the Settings by Device box, find the drop-down menu under Allow List for the device you want to enable. Select Enabled to turn on the Allow List for that device.
7. Make sure that no filter level is applied to this device. If an Allow list is enabled, but no filter is applied, access is restricted to the sites on the Allow list.
8. Click the Save button. You must click the Save button to save the changes to your gateway, or changes will be lost when you navigate away from the page.
9. Log out of the Home Network Manager.

Task: I want to allow access to specific sites blocked by the filter level

You can set up an Allow list to allow access to specific sites that are blocked by the applied filter level.

1. Log in to the Home Network Manager.
2. Click on the Content Filtering link under Basic Services. This opens the Content Filtering summary pane on the right side of the screen.
3. In the table in the Default Settings area, click the Edit Default Lists button. This opens a window where you can enter allowed or blocked website addresses.
4. Type in each website address you want to allow access to, one address per row/line.
    - Use the following format for each website address: www.websitename.xxx (where .xxx is .com, .net, .biz, etcetera).
    - You cannot use http:// or https:// before website addresses.

- If you are allowing a site such as Yahoo or Google, be aware that how you type the address produces different results.
  - www.yahoo.com will allow the front page of Yahoo.com, but will not allow other services such as Yahoo Messenger (messenger.yahoo.com) or Yahoo Mail (mail.yahoo.com).
  - yahoo.com will allow all services from Yahoo.com, including Mail, Messenger, and Flickr.

Formatted: Bullets and Numbering

5. Click OK.
6. In the Settings by Device area, locate the device you want to apply the Allow list to. Choose Enabled from the menu to enable the list for that device.
7. Click the Save button. You must click the Save button to save the changes to your gateway, or changes will be lost when you navigate away from the page.
8. Logout from the Home Network Manager.

Troubleshooting: I can't see a site I expect to see, or I am able to access a site I shouldn't

The interaction among filters and the Allow and Block lists can be complex. Here are some things you can do to troubleshoot content filtering.

If you can't see a site that you think you should be able to:

- Check to see if a filter level that would block the site has been applied to the network or to the specific device. If a filter level is applied, try setting the filter level to None and see if the site is accessible. If the filter is blocking the site, you can add the site to the Allow list and enable the Allow list for the network or a specific device.
- Make sure that the site is not listed on a Block list. If it is, make sure the Block list is disabled in the Default Settings and for the device you are using. (It may be enabled for another device.)
- Make sure that the device does not have an Allow list enabled and no filter level specified. In this case, only sites on the Allow list are accessible.
- Make sure that time blocking is not enabled for the device.

If you can see a site that you think you shouldn't be able to:

- Check to see if a filter level has been applied to the device. You can also try changing the filter level to see if it blocks the site.
- If you have added the site to the Block list, make sure the Block list is enabled for that device.
- To make sure that the site is blocked, add it to the Block list and make sure the Block list is enabled for the network (to block everybody) or for the specific device.

When a device requests access to a site, it does the following in this order:

1. Checks to see if a Block list is enabled. If the site is on the Block list, access is blocked.

2. Checks to see if time blocking is enabled. If the time-blocking settings do not allow access at the current time, access is blocked.
3. Checks to see if an Allow list is enabled. If the site is on the Allow list, access is allowed.
4. Checks to see if a filter level is applied to the network or to the device.
    - If no filter level has been applied, but an Allow list is active, access is not allowed unless the address is on the Allow list.
    - If a category filter has been applied, the device sends the site address (URL) to the content rating service. The content rating service returns information about the category.
        - If the site is in a category banned by the filter, access is blocked.
        - If the site is not in a category banned by the filter or is unrated, access is allowed.
        - If the 6 and Under filter category is applied, access is allowed only if the site is rated as appropriate for children 6 and under.

Port Forwarding

A powerful feature of the Home Network Manager is the ability to remotely configure port forwarding settings for specific network elements connected behind the gateway of the local area network (LAN). Port forwarding is usually necessary to play online games or deploy VoIP services behind a NAT enabled gateway.

Figure 12: Default view of the Port Forwards Summary in the Basic Services area

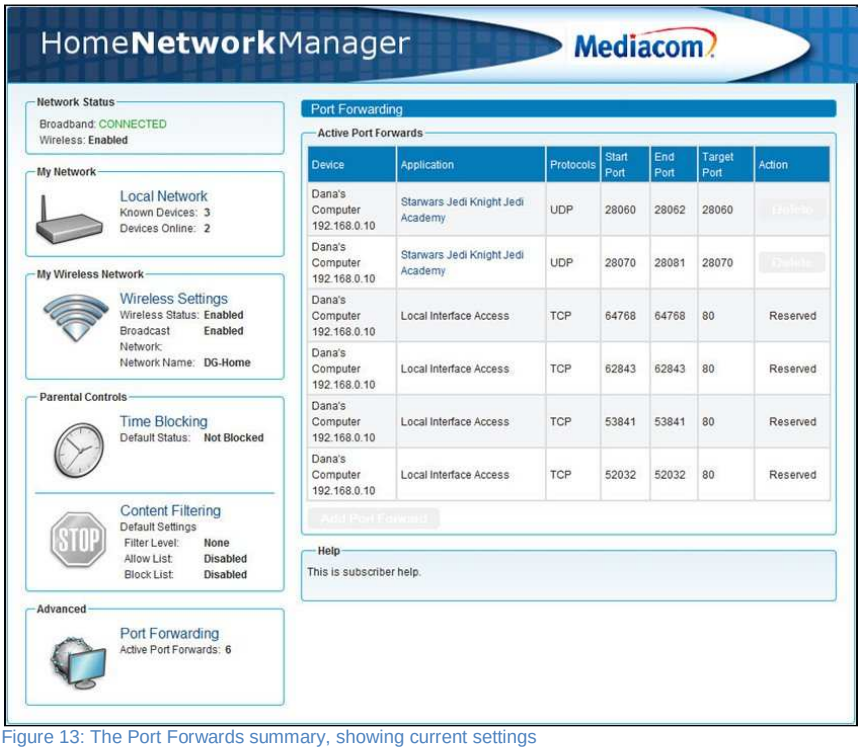


Figure 13: The Port Forwards summary, showing current settings

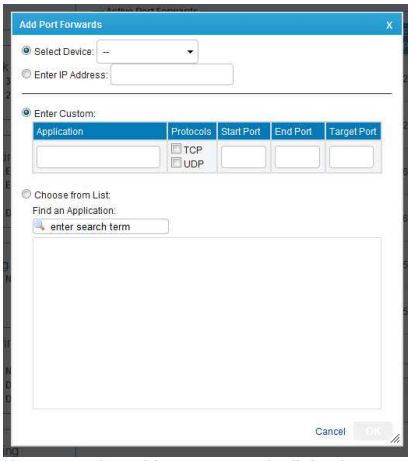


Figure 14: The Add Port Forwards dialog box

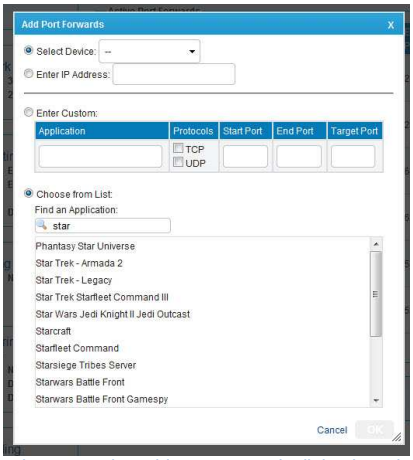


Figure 15: The Add Port Forwards dialog box showing a search

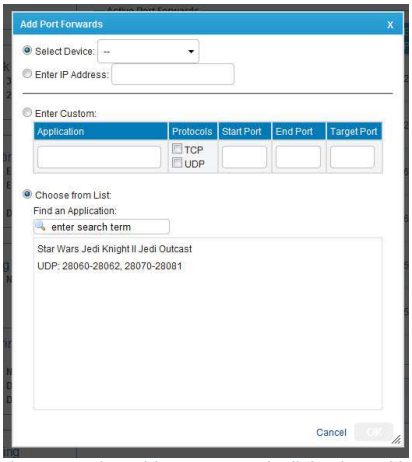


Figure 16: The Add Port Forwards dialog box with a selected application

How to configure Port Forwarding via the Home Network Manager

1. Login into the Home Network Manager.
2. Click on the Port Forwarding link under Advanced. This opens the Port Forwarding summary pane on the right side of the screen.
3. Click on Add Port Forward, which opens up the Add Port Forward dialog box.

4. Choose a host device from the drop-down list, or enter a specific IP address. Note you can only assign port forwards to devices which are currently online.
5. Enter custom settings, or use the search function to find a specific application.
    a. Type the desired application name in the search box – you must enter at least three characters of the application name. This will bring up a list of matching applications.
    b. Click on the desired application.
    c. The search results pane will then show the ports for that application.
6. Click the OK button.
7. Click the Save button. You must click the Save button in order to save the changes to your gateway, or changes will be lost when you navigate away from the page.
8. Logout from the Home Network Manager.
9. The Port Forwarding setting will start working immediately for the application(s) on the selected device.

Task: Creating a Custom Port Forwarding Application Profile

If an application is not listed in the available application profiles, then you can set the port forwarding for that application manually by following the steps below.

1. Login into the Home Network Manager.
2. Click on the Port Forwarding link under Advanced. This opens the Port Forwarding summary pane on the right side of the screen.
3. Click on the Add Port Forward button.
4. Choose a host device from the drop-down list, or enter a specific IP address. Note you can only assign port forwards to devices which are currently online.
5. Type the application name in the Application text box.
6. Select the radio button for Enter Custom.
7. Type the application name in the Application text box.
8. Select either UDP or TCP from the Protocol check boxes.
9. Enter the Port number (or first Port in the range of Ports you are trying to forward) as the Start port. e.g. 2200
10. If you are configuring port forwarding for just one port, then enter the same Start Port as End Port. If you are configuring a range of ports, then enter the final port on the range as the End Port, e.g. 5000
11. Enter the Target Port, which will usually be the first Port in the range.
12. Click the Add button. If the new custom port forward conflicts with any other application profiles added, you cannot save the port forward. Click the cancel button to clear the fields and start over.
13. Click on the OK button.

14. Click on the Save button. You must click the Save button in order to save the changes to your gateway, or changes will be lost when you navigate away from the page.
15. Logout from the Home Network Manager.

Task: I am trying to play an online game with my xBox and get an MTU message

You need to add a Port Forwarding rule to configure the gateway's firewall to map a particular TCP or UDP port (or range of ports) to the Xbox for that application. Port forwarding is usually necessary to play online games.

1. Login into the Home Network Manager.
2. Click on the Port Forwarding link under Advanced. This opens the Port Forwarding summary pane on the right side of the screen.
3. Click on Add Port Forward, which opens up the Add Port Forward dialog box.
4. Choose a host device from the drop-down list, or enter a specific IP address.
5. Enter custom settings, or use the search function to find a specific application.
    a. Type the desired application name in the search box – you must enter at least three characters of the application name. This will bring up a list of matching applications.
    b. Click on the desired application.
    c. The search results pane will then show the ports for that application.
6. Click the OK button.
7. Click the Save button. You must click the Save button in order to save the changes to your gateway, or changes will be lost when you navigate away from the page.
8. Logout from the Home Network Manager

    The Port Forwarding setting will start working immediately for that application on the selected device.