Table of Contents

Overview ......................................................................................................................... 1

Hardware Requirements .................................................................................................. 2
  Cox Business Internet Customers with Dynamic Internet Addresses ......................... 2
  Cox Business Fiber Customers with Static Internet Addresses .................................. 2

Login to MalBlock ............................................................................................................ 3

MalBlock DNS Security Landing Page ............................................................................ 4

Navigating the MalBlock Dashboard ................................................................................ 5

Adding a Static IP Address (for Bring-Your-Own-Bandwidth Users) .......................... 6
  How to Add or Change an IP Address ............................................................................ 6
  How to Remove an IP address ....................................................................................... 8

Validating Your MalBlock Service .................................................................................. 10
  Check Your Device ........................................................................................................ 11
  Malware & Phishing ...................................................................................................... 12
  Botnet ............................................................................................................................ 13

Tracking Security Issues and Analyzing Reports ............................................................. 14

Usage Statistics ................................................................................................................ 14

Device Groups (Premium Subscription Service only) ...................................................... 18

Customizing a Page for Blocked Content ...................................................................... 19

Customizing Pages for Global URL Filtering or Malware and Phishing ..................... 20

Subscribing to Scheduled Reports ................................................................................... 22

Block & Allow Lists ......................................................................................................... 24

Blocking Content by URL (Standard Service) ................................................................. 25

Blocking Content for User Groups (Premium Subscription Service Only) .................. 26

How to Assign Devices to User Groups ....................................................................... 26
  How to Edit an Assigned Device .................................................................................. 27

How to Block Content by Category (Premium Service Only) ........................................ 29

How to Block Content by URL ....................................................................................... 31

How to Bulk Upload a CSV File ...................................................................................... 33

How to Block Content by Schedule .............................................................................. 34
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unblocking a Website</td>
<td>35</td>
</tr>
<tr>
<td>How to Check the Status of a Site</td>
<td>35</td>
</tr>
<tr>
<td>How to Check Protection and Restriction Options (Premium Subscription Service only)</td>
<td>37</td>
</tr>
<tr>
<td>How to Allow Content for a Category</td>
<td>38</td>
</tr>
<tr>
<td>Changing Restrictions for Unrecognized Devices (Premium Service Only)</td>
<td>40</td>
</tr>
<tr>
<td>Turning Web Filters On and Off</td>
<td>41</td>
</tr>
<tr>
<td>Troubleshooting</td>
<td>42</td>
</tr>
<tr>
<td>Windows Clients</td>
<td>44</td>
</tr>
<tr>
<td>MAC Clients</td>
<td>46</td>
</tr>
<tr>
<td>Static DNS Settings</td>
<td>48</td>
</tr>
</tbody>
</table>
Overview

Cox Business MalBlock DNS Security ("MalBlock") is a defense in depth, zero-install, cloud-based service that protects all Local Area Network (LAN) devices by blocking Domain Name System (DNS) lookups for malicious sites. MalBlock also offers a premium upgrade that provides Web Content Filtering, which restricts access to undesirable categories, such as adult content, hacking, violence, social media, and others.

- **Important:** MalBlock cannot clean or remove malware from a device already infected.
- **Refer to the Best Practices and Threat Remediation Guide for the recommended approach to protect your business and to recover quickly from security incidents.**

This guide provides instructions on how to configure security, and content filter settings (for premium users).

![Note: MalBlock Standard and MalBlock Premium provide essential DNS protection functionality.](image)

<table>
<thead>
<tr>
<th>Feature</th>
<th>Standard</th>
<th>Premium</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group Settings</td>
<td>Single</td>
<td>Multiple</td>
<td>Quantity of user groups for unique policy enforcement.</td>
</tr>
<tr>
<td>Malicious Domain Protection</td>
<td>✓</td>
<td>✓</td>
<td>Malware, Ransomware, Phishing &amp; Botnets</td>
</tr>
<tr>
<td>URL Filtering</td>
<td>✓</td>
<td>✓</td>
<td>Internet off, Block and Allowed Individual Domains.</td>
</tr>
<tr>
<td>Google &amp; Bing Safe Search, YouTube Restricted Mode</td>
<td>✓</td>
<td>✓</td>
<td>Block inappropriate or explicit content from search results.</td>
</tr>
<tr>
<td>Web Portal / Dashboard</td>
<td>✓</td>
<td>✓</td>
<td>The Dashboard page shows blocking history details for web filtering, malware, and botnets</td>
</tr>
<tr>
<td>E-mail Reports</td>
<td>✓</td>
<td>✓</td>
<td>Subscribe to Daily, Weekly or Monthly reports sent via e-mail. Provides awareness of unusual activity indicating a potential malware infection.</td>
</tr>
<tr>
<td>Web Content Filtering</td>
<td></td>
<td>✓</td>
<td>Block or Allow by predefined Categories; e.g., hacking, adult content, social media, etc.</td>
</tr>
<tr>
<td>Device Asset Inventory</td>
<td></td>
<td>✓</td>
<td>Catalog LAN devices by MAC Address for unique protections and restrictions.</td>
</tr>
</tbody>
</table>

**MalBlock Premium** adds two features: **Web Content Filtering** based on content categories and **Device Inventory** for asset tracking and management.
**Hardware Requirements**

**Cox Business Internet Customers with Dynamic Internet Addresses**

- Certified Cox Business Modem. Use the following link to confirm:
  - Modem should be in gateway mode (non-bridged mode)\(^1\).

**Cox Business Fiber Customers with Static Internet Addresses**

- A locally connected router that provides users on the customer's network with local IP addresses via Dynamic Host Configuration Protocol (DHCP).

---

\(^1\)A gateway connects the Internet with your local area network. This is the default configuration of Cox supplied gateways and modems. Customers with their own gateway/firewall may put their modem in bridge mode to bypass the gateway in the modem.
Login to MalBlock

You can access MalBlock through the MyAccount portal.

**Figure 1. MyAccount Login screen**

![MyAccount Login screen](image)

Use the following steps to access the MalBlock service.

1. Enter [myaccount.coxbusiness.com](http://myaccount.coxbusiness.com) in your web browser.
2. Enter your MyAccount **User ID** and **Password** and click the **Sign In** button.
3. From the Welcome page, scroll to the My Services section. *(Note: If there are multiple accounts, select the one with MalBlock service then proceed to step 4.)*
4. Click the **Internet** tab and the **MalBlock DNS Security** icon.
   **Result:** The MalBlock DNS Security screen appears. *(See Figure 3.)*

**Figure 2. MyAccount Welcome screen**

![MyAccount Welcome screen](image)
MalBlock DNS Security Landing Page

The MalBlock DNS Security main page allows you to: change or review DNS security options, view, delete, or add a static IP*, check that your connected devices are safe, view detailed information about any malware, phishing or botnets that have been blocked, and confirm that web content categories are filtered** appropriately.

Figure 3. **MalBlock DNS Security screen**

*The Static IP Address button appears only if you have purchased MalBlock and are not in a Cox Business franchise location served with any Cox Internet service.

**The Web Content Filtering button appears only with Premium service.
Navigating the MalBlock Dashboard

The MalBlock Dashboard allows you to:

- change or review your DNS security options
- add a device (to be protected)
- specify a timeframe in which you want to capture data
- view usage statistics and details about URL filters, Malware/Phishing, and Botnets that have been blocked
- see Internet activity, global URL filter blocks, and malware and phishing blocked by Group, New Devices, and Employees*
- view status and details of devices that are new (unsaved), infected, and blocked

Figure 4. MalBlock Dashboard

Use the following steps to view the Dashboard.

1. Login to MalBlock.
   Result: The MalBlock DNS Security screen appears.

2. Scroll down the page and click the MalBlock Dashboard button.
   Result: The Dashboard appears. (See Figure 4.)

*Groups are only visible with Premium service.
3. Click the **See More** button under the Global URL Filter Blocks, Malware and Phishing Blocked, and Botnet Blocked sections to see details of each and download as a .CSV file for analysis, if desired.

**Adding a Static IP Address (for Bring-Your-Own-Bandwidth Users)**

If you are not in one of Cox Business’s franchise locations and are not served by any Cox Internet service, you must have a static IP address with another provider before you can use MalBlock.

If you have multiple static IPs or want to make a change to your account, you may need to add or change your IP address(es). The MalBlock service can support up to two IP addresses.

**How to Add or Change an IP Address**

**Figure 6. MalBlock IP Address Management screen**

Use the following steps to add, view, and delete a static IP address.
1. Login to MyAccount and access the MalBlock DNS Security portal.  
   **Result:** The MalBlock DNS Security screen appears.

2. Click the **Static IP Address** button. (See Figure 3.)  
   **Result:** The MalBlock IP Address Management screen appears. (See Figure 6.)

3. Click the **Add IP Address** link.  
   **Result:** The Add IP Address dialog box appears.

   **Figure 7.** Select IP Type dialog box

   ![Select IP Type dialog box](image)

4. Click the **Select IP Type** drop down menu and select the IPv4 or IPv6 option.  
   **Result:** A second Add IP Address dialog box appears.

   **Figure 8.** Enter IP Address dialog box

   ![Enter IP Address dialog box](image)

5. Enter and re-enter the **Static IP Address** (for the IP type you selected) in the fields provided.

6. Click the **Confirm** button.  
   **Result:** The new IP address is added to the list.
How to Remove an IP address

Use the following steps to delete a static IP address.

1. **Login to MyAccount and access the MalBlock DNS Security portal.**
   **Result:** The MalBlock DNS Security screen appears.

2. **Click the Static IP Address button.** (See Figure 3.)
   **Result:** The MalBlock IP Address Management screen appears.

3. Click the trash can icon to the right of the IP address you want to remove.
   **Result:** A Warning dialog box appears.
Figure 11. **Warning dialog box**

![Warning dialog box](image)

4. If you want to proceed with the deletion, click the **Yes** button. Click the **No** button to cancel.
Validating Your MalBlock Service

MalBlock prevents malware, phishing, and botnets. It also protects your network if your public IP address is provisioned correctly. Click the **Check Your Device, Malware & Phishing, Botnet, and Web Content Filtering** buttons in Figure 12 to confirm that each pre-defined Web category is filtered properly. Each blocked category includes a counter that is updated in the MalBlock Dashboard.

**Figure 12. MalBlock Security screen**

---

MalBlock DNS Security Landing Page

---

Cox Business MalBlock User Guide
Check Your Device

Use the following steps to confirm that your device is protected.

1. Login to MyAccount and access the MalBlock DNS Security portal.  
Result: The MalBlock DNS Security screen appears.

2. Click the Check Your Device button. (See Figure 3.)  
Result: The MalBlock DNS Security Protection Check screen appears. If the service is configured incorrectly, the Protection Check page will indicate that your device is not protected. Validate your settings and refer to the Troubleshooting section for more information.

Figure 13. Check Your Device – Not Protected status

If the service is configured correctly, a green check mark will indicate that your device is protected.

Figure 14. Check Your Device – Protected status
Malware & Phishing

Use the following steps to confirm that your device is protected against malware and phishing attacks.

1. Login to MyAccount and access the MalBlock DNS Security portal. **Result:** The MalBlock DNS Security screen appears.

2. Click the **Malware & Phishing** button. (See Figure 3.) **Result:** The MalBlock DNS Security Protection Check screen appears. You will see a message that states your device is protected or is not protected from malware and phishing. Validate your settings and refer to the **Troubleshooting** section for more information.

**Figure 15. Malware & Phishing validation screen**

![Malware & Phishing validation screen](image-url)
Botnet

Use the following steps to confirm that your device is protected against botnet attacks.

1. Login to MyAccount and access the MalBlock DNS Security portal. 
   **Result:** The MalBlock DNS Security screen appears.

2. Click the  **Botnet** button. (See Figure 3.)
   **Result:** The MalBlock DNS Security Protection Check screen appears. You will see a message that states your device is protected or is not protected from botnets. Validate your settings and refer to the  *Troubleshooting* section for more information.

**Figure 16. Botnet validation screen**
Tracking Security Issues and Analyzing Reports

Once you validate that MalBlock is preventing threats, you can track and analyze security issues through the MalBlock Dashboard.

Cox Business regularly reviews existing and new threats on the Internet, and takes swift action to block malware, phishing, and botnet attacks at the DNS level. The data science team updates the Threat List daily.

**Usage Statistics**

MalBlock depicts the actions that have been used to enforce Web Filter, Malware, Phishing, and Botnet protection for your network. You can filter the timeframe that data is captured. The options are 24 hours, 7 days, or 30 days.

*Note:* *Only subscribers with MalBlock Premium can view.*

![Figure 17. MalBlock Dashboard – Usage Statistics](image)

Refer to the steps in the *Navigating the MalBlock Dashboard* section to access the Usage Statistics screen.

Click the **See More** button under each category to see details such as URLs blocked, their category* or threat type, date, number of times blocked, and devices on which the URLs were blocked.
• **Blocked by Web Filter**: Displays how many times network users attempted to access content in blocked categories. *(Note: Categories are only shown for premium subscribers.)*

---

**Figure 19. Global URL Filter Blocks screen**

<table>
<thead>
<tr>
<th>URL</th>
<th>Reason</th>
<th>Category</th>
<th>Device Name/ID</th>
<th>Time Period</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="https://gla.houseparty.com/">https://gla.houseparty.com/</a></td>
<td>Medium</td>
<td>Entertainment</td>
<td>Unknown</td>
<td>Nov 06, 2019 05:15 PM - 06:00 PM</td>
<td>6</td>
</tr>
<tr>
<td><a href="https://tap.turoc.apple.com">https://tap.turoc.apple.com</a></td>
<td>Medium</td>
<td>Entertainment</td>
<td>Unknown</td>
<td>Nov 06, 2019 06:15 PM - 07:00 PM</td>
<td>3</td>
</tr>
</tbody>
</table>
• **Malware & Phishing Blocked**: Displays how many phishing and malicious software attacks were blocked.
  
  o **Severity/Type (shown for Botnet blocks)**: The type of threat and its severity.
  
  o **Severity levels are indicated by color-coded dots next to the Threat Type name.**
    
    ▪ **Low-medium severity: grey**
      
      Includes adware, unwanted software that may have been bundled in with another download, etc.
    
    ▪ **Medium severity: blue**
      
      Includes threats such as phishing attacks, spambots, browser hijacking malware, etc.
    
    ▪ **High severity: orange**
      
      Includes threats such as banking trojans, spyware that steals user data, credential theft, etc.
    
    ▪ **Highest Severity (Critical): red**
      
      Includes threats such as ransomware that encrypts all files on a computer, data exfiltration attacks, keyloggers and more.
  
• **Botnet Blocked**: Displays the number of blocked attempts to access network devices in automatic (unauthorized) mode from outside your network.

**Figure 20. Standard Subscription Service View**
Figure 21. **Premium Subscription Service View with Device Groups**

![Premium Subscription Service View with Device Groups](image-url)

- Internet Activity
- Global URL Filter Blocks
- Malware and Phishing Blocked

*Certain websites and apps remain active in the background even when not directly in use*
Device Groups (Premium Subscription Service only)

In a Multiple Group Settings configuration, MalBlock lists network devices that need to be addressed. You can identify the device by name and MAC address to determine the status of the device on your network. Refer to How to Assign Devices to User Groups for steps on how to assign devices to groups.

Figure 22. Network Devices status

- New Devices (Unsaved): New and unrecognized devices in your network appear in the New Devices (Unsaved) group. MalBlock displays only currently active devices. You can block unwanted devices or change the users’ access and protection levels by assigning their devices to groups.

- Infected Devices: Displays network devices infected in the last 24 hours. You can see infection type and block any infected device.

- Blocked Devices: Displays unwanted and infected devices that you blocked. You can unblock the devices.
Customizing a Page for Blocked Content

A specific page, known as a “Blocked page” appears when users in your network attempt to view a restricted website or if the content poses a malware or phishing risk. You can customize the message with branding, inform the user why the page is blocked, and provide contact information if the user has questions.

Figure 23. Block Page Customization – General Branding

Use the following steps to customize the icon, ink color, insert a logo, and create a message that the user will see on the block page.

1. Login to MyAccount and access the MalBlock DNS Security portal. **Result:** The MalBlock DNS Security screen appears.
2. Click the MalBlock Dashboard button.
3. Click the **Block Page Customization** tab and the **General Branding** link. **Result:** The page customization options screen appears.
4. Enter a message (140 character max) in the **Title** field. Upload a logo to display next to the message if desired. Refer to the specifications to ensure the logo will fit.
5. **IMPORTANT:** Click the **Save changes** button before you proceed to the Global URL Filtering tab or Malware and Phishing tab. If you click another tab before you **Save**, you will lose any changes you made.
Customizing Pages for Global URL Filtering or Malware and Phishing

The Global URL Filtering and Malware and Phishing sections can also be customized for alert messages that display when Web Filters or Malware and Phishing protection block a website.

Figure 24.  Global URL Filtering

Use the following steps to customize the block page.

1. Login to MyAccount and access the MalBlock DNS Security portal.  
   Result: The MalBlock DNS Security screen appears.

2. Click the MalBlock Dashboard button.

3. Click the Block Page Customization tab and the Global URL Filtering or Malware and Phishing link.  
   Result: The page customization options screen appears.

4. Check the Show a blocking reason message box to enter a message that will appear when someone attempts to access a blocked website.

5. Enter the message that the viewer will see in the text field.
6. (Optional) Enter the **Admin’s Email** and **Admin’s Phone Number** to display an administrator’s contact information in the block message.

7. The Global URL Filtering block page in a Multiple Group Settings configuration (Premium Only), allows you to choose how network users may ask for registration of their new device: via a **4 character code**, a **Device Name**, or both. MalBlock displays the options for people who use device registration.

8. **IMPORTANT**: Click the **Save changes** button before you proceed to the General Branding tab or Malware and Phishing tab. If you click another tab before you **Save**, you will lose any changes you made.
Subscribing to Scheduled Reports

If you do not want to log in to MalBlock to check security reports, or if another person does not have a MalBlock login, you can add your email and the other person’s email to receive reports. (Note: The reports contain the numbers that you see for the usage statistics on the Dashboard page.)

Figure 25. Scheduled Reports screen

- **Blocked by Web Filter**: Displays the number of times network users have attempted to access content in blocked categories.
- **Malware & Phishing Blocked**: Displays how many phishing and malicious software attacks have been blocked.
- **Botnet Blocked**: Displays the number of blocked attempts to access network devices in automatic (unauthorized) mode external to your network.
- **Total DNS Requests**: Total number DNS requests during your selected time period
- **Malicious Requests**: Sum of malware & phishing and botnet blocks during your selected time period

The data is aggregated by day, week, or month according to the email frequency you specify when subscribing to the reports.
Use the following steps to receive schedule usage reports.

1. Login to MyAccount and access the MalBlock DNS Security portal.  
   **Result:** The MalBlock DNS Security screen appears.

2. Click the **MalBlock Dashboard** button.

3. Click the **Scheduled Reports** tab.  
   **Result:** The page customization options screen appears.

4. Enter your **Email** or another person’s email address and select the **Frequency** (Never, Daily, Weekly, Monthly) with which you want to receive reports.

5. Click the **Save** button.
Block & Allow Lists

The Block & Allow Lists page lets you make lists of specific web sites or URLs that you want to block or allow access to. These sites are in addition to any sites already in the web filters settings.

- **Specific URL.** Specific URLs take two formats. They can be subdomains, or they can be domains with paths. For example, “www.coxbusiness.com” and “akamai.com/news” are both considered “specific URLs” for this application.

  If you type a URL into the check box, as in the example above, the application will show you two choices. You will be asked if you want to block the whole website or just that specific URL. If you block the whole website, any variation of the URL, including subdomains or paths, will be blocked. If you choose to block the specific URL, only the URL you entered will be blocked. So, for example, “www.coxbusiness.com” will be blocked, but “news.akamai.com” will be allowed.

  It is not possible to add a specific URL to the allow list.

  If you have a website on the allow list, such as “www.coxbusiness.com”, you can add a URL to the block list, but it won’t be blocked because the allow list will be processed first.

- **Whole website.** “Whole website” is the term used to refer to everything related to a specific core domain. (A core domain is usually a Second Level Domain, such as “akamai.com”.) Whole websites are the only type of site that can be added to the allow list. They may also be blocked.

- **TLD.** A Top Level Domain (or TLD) may be blocked. Doing so causes every domain under that TLD to be blocked! An example of a TLD is “com”. “Public suffix” sites, such as “co.uk” are treated as TLDs.

  TLDs may not be added to the Allow list. TLDs may not be uploaded in CSV files. When entering TLDs, do not use beginning or ending “dots”; that is, “.com” and “com.” will be rejected. Also, do not use wildcards; “*.com” will be rejected.

  Because blocking a TLD may cause some services to break, there is a special second confirmation check on requests to block TLDs.

  Note that you will always retain access to the portal itself, even if you block the TLD under which it resides.

  The Allow list takes precedent over the Block list.
Use the following steps to block content from a specific URL.

1. Login to MyAccount and access the MalBlock DNS Security portal. **Result:** The MalBlock DNS Security screen appears.

2. Click the **MalBlock Dashboard** button.

3. Click the **Settings** tab to expand and select the **Block and Allow Lists** option. **Result:** The window by the same name appears.

4. Enter a URL in the text field and click the **Check** button. **Result:** A second screen appears and prompts you to select the radio button for either the **Whole website** or **Only this specific URL**. (Note: It is not possible to add specific URLs to the Allow list.)

5. Click the **Block** or **Allow** button based on your business requirements. **Result:** The URL appears in the appropriate category. (Note: To remove a URL from either the Block or Allow list, click the icon to the left of the URL.)
Blocking Content for User Groups (Premium Subscription Service Only)

You can allow or block categories of content for user groups according to a schedule you set up. You can also allow or block access to certain websites for selected user groups only or across your entire network.

How to Assign Devices to User Groups

MalBlock identifies devices (computers, tablets, and phones) in your network by their MAC Address. Your network must have dnsmasq to support multiple user groups with assigned devices. For more information about dnsmasq and how to setup and configure it, refer to the Dnsmasq Configuration Guide.

In a Single Group Setting configuration, only one group governs protection and restriction for devices in your network. In a Multiple Group Settings configuration, you can change protection and restriction for devices by assigning devices to different groups. New and unregistered devices in your network are automatically protected and restricted by the New Devices (Unsaved) user group. You can block devices or assign them to another group. If you do not recognize a new device and do not want to block it, the user of the device may ask you to change device restrictions.

Figure 28. Settings: Devices tab

Use the following steps to assign new and unregistered devices.

1. Login to MyAccount and access the MalBlock DNS Security portal. **Result:** The MalBlock DNS Security screen appears.
2. Click the MalBlock Dashboard button.
3. Click the Settings tab to expand and select the Devices option.
4. Select the New Devices (Unsaved) link to change the restriction status of devices. Select the Online Devices link for unregistered devices active in the network during the last hour.
5. Click the plus sign (+) in the Actions column to assign a device.
How to Edit an Assigned Device

This section instructs you on how to assign devices to different groups.

1. Login to MyAccount and access the MalBlock DNS Security portal. **Result:** The MalBlock DNS Security screen appears.
2. Click the MalBlock Dashboard button.
3. Click the Settings tab to expand and select the Devices option.
4. Choose a user group other than New Devices (Unsaved) and select a device from the list to reassign.
5. Click the Edit icon (the pencil).
6. Choose another user group for the device. (Note: You can also use the MAC Address to add a device directly to a user group.)

7. Click the **Add Device** button in the top toolbar.

8. Enter the **4 Character Code** and **Device Name** in the fields.

**Figure 31. Add Device screen**

![Add Device screen]

9. Click the **Add Device** button.

**Result:** The newly paired Group and Device appear as a new line item in the list. See Figure 32.

**Figure 32. Reassign Device to Group list**

![Reassign Device to Group list]
How to Block Content by Category (Premium Service Only)

MalBlock enables you to block sites or categories for some employees while allowing access to the sites for other employees.

The easiest way to block sites for all employees is to choose the Employees user group and assign one of the default filters (Light, Medium, and Strict) to them. This will bar a category of sites for the entire group. If you want some employees to access the site, you will need to create a new user group and assign different filters.

If none of the default filters are suitable, you can create a Custom filter. (See Figure 34.)

Use the following steps to create a custom filter.

1. Select one of the default filters.
2. When you have checked or unchecked any category, click the Custom button to save that template.
3. If you want limited employees to have access to hacking sites, add a new user group and assign different filters to each.

Figure 33. **Settings: Protection Preferences**

Use the following steps to block or allow access to categories for groups of users.

1. Login to MyAccount and access the MalBlock DNS Security portal. **Result**: The MalBlock DNS Security screen appears.
2. Click the **MalBlock Dashboard** button.
3. Click the **Settings** tab to expand and select the **Protection Preferences** option.
4. Select the User Group **Employees**.
5. From the Protection Level list, apply the filter type of your choice. 
   **Result:** The user group will be assigned that protection level. *(Note: Click the Block All or Allow All categories to apply a “blanket” filter.)*

**Figure 34. Protection Level**
How to Block Content by URL

You can block access to a single website either for selected user groups or across your entire network. It is helpful if you do not want to restrict access to an entire category of sites, or if the existing category does not contain the site you want to block.

Figure 35. **Block and Allows Lists screen**

Use the following steps to block content by URL.

1. Login to MyAccount and access the MalBlock DNS Security portal. **Result:** The MalBlock DNS Security screen appears.
2. Click the **MalBlock Dashboard** button.
3. Click the **Settings** tab to expand and click the **Block and Allow Lists** option.
4. Enter the URL in the text field and click the **Check** button to see its status. (**Note:** You may be prompted to choose how you want to block (or allow) the URL. It can be the URL path only, the core domain, or the core domain with subdomains; e.g., google.com/feed/login, google.com, maps.google.com, or other Google subdomains. The number of choices may vary.)
5. To confirm your choice and blacklist the URL, click the **Block** button. **Result:** When a URL is blacklisted, the content is unavailable to selected user groups regardless of the group’s filtering levels.
Figure 36. **Block Content by URL screen**

- **Global**
  - Applies to all the groups
- **New Devices (Unsaved)**
  - Default group for new users
- **Employees**
  - Trusted users

**Manage your Block & Allow lists associated with the selected group**

- **casino.com**
  - The allow list has a higher priority, so subdomains from the block list will not be blocked if their core domains are allow listed.

Select the path you want to block or allow:

- **Whole website: casino.com**

**Block list**
- No URL in this list
**Remove All**
**Allow list**
- No URL in this list
**Remove All**
How to Bulk Upload a CSV File

You can upload a bulk Block or Allow list as a .CSV file; however, the file must be formatted with a new domain per row in a single column before you can upload. The Block list and Allow list each supports up to ten entries per group. Entries processed by file upload are domain level only and any URL paths are ignored on upload.

Use the following steps to upload a bulk Block or Allow file.

1. Create a .CSV list for the sites you want to block or allow. (Note: A file cannot have a list with allow and block types.) The text file below (named whitelist.csv) contains two domains that will be added to the allow list.

   ![whitelist - Notepad](image)

   ```csv
   coxbusiness.com
googlr.com
   ```

2. Login to MyAccount and access the MalBlock DNS Security portal.
   **Result:** The MalBlock DNS Security screen appears.

3. Click the MalBlock Dashboard button.

4. Click the Settings tab to expand and click the Block and Allow Lists option.

5. Click the Upload List (.csv) button.

6. Click the Choose file… button.

7. Locate the .CSV file and click the Open button., you are prompted to Block or Allow the sites. (See Figure 36.)

8. Click the Allow button.
   **Result:** The domains are added to the corresponding list.

Figure 37. Bulk File Upload
How to Block Content by Schedule

MalBlock enables you to restrict access to content based on the day of the week and time of day.

Figure 38. Block Content by Schedule

Use the following steps to establish times that content will be unrestricted.

1. Login to MyAccount and access the MalBlock DNS Security portal.
   Result: The MalBlock DNS Security screen appears.

2. Click the **MalBlock Dashboard** button.

3. Click the **Settings** tab to expand and click the **Protection Preferences** option.

4. Click a User Group to whom you want to allow content access during set hours.

5. Scroll to the **Content Restriction Schedule** and click the toggle to turn **ON**.
   Result: The Create Rule calendar appears.

6. Scroll down to the Web Filter Option section and select which content categories to block. **(Note:** The categories that the web filter blocks for the group are already selected for the schedule. You cannot deselect those categories.)
7. Click the **Create Rule** button and populate the days and times the rule will be in effect.
   **Result:** The Rule will appear in the right navigation panel on the calendar. You can edit or remove the rule by clicking the corresponding icon.

8. Click the **Save** button.

### Unblocking a Website

Cox Business encourages the MalBlock administrator to determine why a site is blocked before any restriction is removed. The causes may be that the site belongs to a category that is blocked for the user group or the URL for the site is blacklisted.

### How to Check the Status of a Site

You can check the status of a site (Blocked or Unblocked) for Multiple Group Settings configuration and Single Group Setting configuration.

**Figure 39. Site Status lists for Multiple Group Settings Configurations**

Use the following steps to check the status of a site in a Multiple Group Settings configuration.

1. Login to MyAccount and access the MalBlock DNS Security portal.
   **Result:** The MalBlock DNS Security screen appears.

2. Click the **MalBlock Dashboard** button.

3. Click the **Settings** tab to expand and click the **Block and Allows Lists** option.

4. Select the User Group you want to check the site against and enter its URL in the text field, then click the **Check** button.
   **Result:** The site will appear in either the Block or Allow list.
Use the following steps to check the status of a site in a Single Group Setting configuration.

1. Login to MyAccount and access the MalBlock DNS Security portal. **Result:** The MalBlock DNS Security screen appears.
2. Click the **MalBlock Dashboard** button.
3. Click the **Global URL Filter Blocks** link. **Result:** A list of URLs appears. (**Note:** If the URL is blacklisted, no one in the group has access to it and you can remove it from the list. If you add the URL to the whitelist, you make the website available to all devices of the user group regardless of the filtering levels.)
How to Check Protection and Restriction Options (Premium Subscription Service only)

If a website’s URL is not blacklisted in a Multiple Group Settings configuration, find the group to which the user belongs; and then check the restriction and protection options of the group.

**Figure 41. Multiple Group Settings lookup**

![Multiple Group Settings lookup](image)

Ask the user for the MAC address of the device they use to access the network. Use the following steps to find devices associated to a user group.

1. Login to MyAccount and access the MalBlock DNS Security portal. **Result:** The MalBlock DNS Security screen appears.
2. Click the **MalBlock Dashboard** button.
3. Click the **Settings** tab.
4. Click the **Devices** tab.
5. Identify the MAC address in the available user group(s): *(New Devices (unsaved) and Employees)*.
6. Click the group name to see the MAC address in the Device ID column.

Obtain the following information to identify the setting (in a user group) that blocks a website.

- Ask the user which alert displays when a specific website is blocked
- Ask the day and time the user attempts to access the website. **(Note:** If the alert is Malware and Phishing, the website is blocked by Internet Security. Unblocking such websites is not recommended. If the alert is Website Blocked, a content category in Web Filters or Restrict Content Schedule is likely the cause. In this case, you can allow the category for the user group.

1. Click the **Domain Lookup** tab.
2. Enter the URL of a website in the text field and click the **Search** button. **(Note:** If the alert is Malware and Phishing, the website is blocked by Internet Security. Unblocking such websites is not recommended. If the alert is Website Blocked, a content category in Web Filters or Restrict Content Schedule is likely the cause. In this case, you can allow the category for the user group.

   **Result:** MalBlock searches for the content category to which the site belongs.
How to Allow Content for a Category

Use the following steps to allow content for a category.

1. Login to MyAccount and access the MalBlock DNS Security portal. **Result:** The MalBlock DNS Security screen appears.

2. Click the **MalBlock Dashboard** button.

3. Click the Settings tab and the Protection Preferences option.

4. Select a user group. (See Figure 43.)

Figure 43. **Protection Preferences - Groups**
5. Scroll to the Web Filters section and determine whether a filter blocks the category. If so, click the icon to allow.

Figure 44. **Web Filters**

![Web Filters](image)

6. Scroll to the **Content Restriction Schedule** section. If it is selected, confirm that there are no schedule rules blocking the category.

Figure 45. **Content Restriction Schedule**

![Content Restriction Schedule](image)

7. Scroll to the bottom of the page and click the **Save** button. (Note: You can also allow a content category for the single group in a Single Group Settings configuration. To navigate to the group, click the **Settings** tab from the Dashboard screen.)
Changing Restrictions for Unrecognized Devices (Premium Service Only)

In a Multiple Group Settings configuration, MalBlock uses the restrictions of the New Devices (Unsaved) user group for new and unregistered devices on your network. There are multiple ways to change the restrictions.

- Have a web page blocked on a device due to the restrictions of the group. In this example, people see the Global URL Filtering block page with the options you chose for device registration. To choose the options, including the email for registration requests, customize the block page.

- To see registration requests, place your cursor over the bell alert icon on the top right of the navigation menu. Click any request to switch to the full view of device registration requests.

- To register a device, click the Assign button for the device and choose a user group to which the device should belong. (Note: Alternatively, click the Add Device button and complete the device registration by using the MAC address or the character code from the request. See Figure 47.)

Figure 46. Settings: Devices screen
To identify a device by the code, the device should be either on the network or disconnected within the last 15 minutes.

**Turning Web Filters On and Off**

Web Filters are turned on automatically; and although you can turn them off if necessary, Cox Business recommends that they remain in the **ON** position. By doing this, the following MalBlock settings stay inactive until the time you turn on Web Filters again:

- Protection and restriction settings for each user group according to your saved configuration (this feature is only available in the Premium service tier).
- Blacklists and whitelists that explicitly control access to internet content.
- Malware, phishing and botnet traffic is generated by malicious software. Protection against this traffic is critical. Therefore, Cox Business does **not recommend disabling the Malware and Phishing setting for any user group.** The setting remains enabled even if you turn off Web Filters.

Click the **Web Filters** toggle **OFF** to deactivate them or toggle **ON** to activate. The change is applied immediately.
Troubleshooting

This section instructs you on how to verify a client’s DNS service address on a Windows or Mac PC. For reference, the MalBlock DNS server addresses are:

<table>
<thead>
<tr>
<th>IPv4</th>
<th>IPv6</th>
</tr>
</thead>
<tbody>
<tr>
<td>72.200.254.11</td>
<td>2001:57a:102::11</td>
</tr>
<tr>
<td>72.200.255.11</td>
<td>2001:57a:103::11</td>
</tr>
</tbody>
</table>

The addresses are automatically configured when your router and PC accept the MalBlock DNS servers offered by the Cox network DHCP server. The illustration below depicts the setup where:

- The broadband gateway or router local IP address is 192.168.1.1.
- The gateway/router and LAN clients accept the MalBlock DNS servers offered by the Cox network.

*Figure 48. Broadband Gateway/Router with DHCP Enabled*
If you have a Linksys WiFi router, the configuration would match the setup in Figure 49 where DHCP is enabled on the router WAN (Internet) and LAN interface, and Static DNS is not configured (all zeros, 0.0.0.0).

**Figure 49. Linksys Router – Static DNS Not Configured**
Troubleshooting

Windows Clients

If you are a Windows user, follow the steps below to view the DNS Server IP address(es) configured on your PC and confirm these are the MalBlock DNS servers.

1. Press the **Windows+R** keys to open a Run box.

2. Enter `cmd` and click the **OK** button or press the **Enter** key.

3. Type `ipconfig /all` and press the **Enter** key.

The output will vary depending on the number of wired- and wireless Ethernet adapters on your PC. The MalBlock DNS servers are highlighted in the results:

```
C:\>ipconfig /all
Windows IP Configuration

    Host Name . . . . . . . . . . . . : Dell
    Primary Dns Suffix . . . . . . . . . . . : 
    Node Type . . . . . . . . . . . . : Hybrid
    IP Routing Enabled. . . . . . . . . . . . : No
    WINS Proxy Enabled. . . . . . . . . . . . : No
    DNS Suffix Search List. . . . . . . . : mc.at.cox.net.
```

<additional adapters omitted for brevity>
Ethernet adapter Ethernet:

- Connection-specific DNS Suffix: mc.at.cox.net.
- Description: Intel(R) Ethernet Connection (7) I219-LM
- Physical Address: 8C-04-BA-02-65-AB
- DHCP Enabled: Yes
- Autoconfiguration Enabled: Yes
- Link-local IPv6 Address: fe80::4846:20a3:30f1:2a97%11(Preferred)
- IPv4 Address: 192.168.1.100(Preferred)
- Subnet Mask: 255.255.255.0
- Lease Obtained: Sunday, November 10, 2019 3:35:10 PM
- Lease Expires: Monday, November 11, 2019 3:40:25 PM
- Default Gateway: 192.168.1.1
- DHCP Server: 192.168.1.1
- DHCPv6 IAID: 126616762
- DHCPv6 Client DUID: 00-01-00-01-24-FC-97-A1-8C-04-BA-02-65-AB
- DNS Servers: 72.200.254.11 72.200.255.11
- NetBIOS over Tcpip: Enabled

If the PC is connected to WiFi, the MalBlock DNS servers will display in the WiFi adapter:

Wireless LAN adapter Wi-Fi:

- Connection-specific DNS Suffix: Qualcomm QCA61x4A 802.11ac Wireless Adapter
- Physical Address: EC-5C-68-78-04-5F
- DHCP Enabled: Yes
- Autoconfiguration Enabled: Yes
- Link-local IPv6 Address: fe80::355f:cf49:3a1f:b745%6(Preferred)
- IPv4 Address: 192.168.1.101(Preferred)
- Subnet Mask: 255.255.255.0
- Lease Obtained: Sunday, November 10, 2019 12:31:55 PM
- Lease Expires: Monday, November 11, 2019 12:31:56 PM
- Default Gateway: 192.168.1.1
- DHCP Server: 192.168.1.1
- DHCPv6 IAID: 267148392
- DHCPv6 Client DUID: 00-01-00-01-24-FC-97-A1-8C-04-BA-02-65-AB
- DNS Servers: 72.200.254.11 72.200.255.11
- NetBIOS over Tcpip: Enabled
**MAC Clients**

If you are a Mac user, follow the steps below to view the DNS Server address(es) being used on your network.

1. Go to the Apple menu and select **System Preferences**.

2. Choose the **Network** control panel, select your network interface from the left side; e.g., Wi-Fi or Ethernet, then click the **Advanced** button in the lower right corner of the Network window:

3. Choose the **DNS** tab at the top of the screen.
The DNS Servers can also be verified from the Terminal command line:

1. Go to the Apple menu and select **Launchpad**.
2. Open the **Other** folder and select **Terminal**.
3. Type the command `scutil --dns` and press enter.

```
Mac:~ admin$ scutil --dns
DNS configuration

resolver #1
  nameserver[0] : 72.200.254.11
  nameserver[1] : 72.200.255.11
  if_index : 8 (en0)
  flags : Request A records
  reach : 0x00020002 (Reachable,Directly Reachable Address)

resolver #2
  domain : local
  options : mdns
  timeout : 5
  flags : Request A records
  reach : 0x00000000 (Not Reachable)
    - order : 300000

<additional resolvers omitted for brevity>

DNS configuration (for scoped queries)

resolver #1
  nameserver[0] : 72.200.254.11
  nameserver[1] : 72.200.255.11
  if_index : 8 (en0)
  flags : Scoped, Request A records
  reach : 0x00020002 (Reachable,Directly Reachable Address)
**Static DNS Settings**

The network administrator may choose to manually configure the DNS servers, which overrides the settings offered by the Cox DHCP server. As shown in Figure 50, the MalBlock DNS servers are statically configured on the router, which is the local DNS server for LAN clients. In this mode, the LAN clients forward DNS lookups to the gateway/router DNS server at 192.168.2.1, which then forwards lookups to the MalBlock servers.

![Figure 50. Linksys Router – Static DNS Configured](image)

The corresponding Linksys router configuration is illustrated in Figure 51 on page 49.
Figure 51. **Linksys Router – MalBlock Static DNS**

On Windows, the `ipconfig /all` command now displays the Linksys router DNS server IP address of 192.168.1.2 instead of the MalBlock server IPs:

C:\>ipconfig /all

Windows IP Configuration

- Host Name . . . . . . . . . . . . . . . : Dell
- Primary Dns Suffix . . . . . . . . . : 
- Node Type . . . . . . . . . . . . . . . : Hybrid
- IP Routing Enabled. . . . . . . . . : No
- WINS Proxy Enabled. . . . . . . . : No
- DNS Suffix Search List. . . . . . . : mc.at.cox.net.
**Ethernet adapter Ethernet:**

- **Connection-specific DNS Suffix**: mc.at.cox.net.
- **Description**: Intel(R) Ethernet Connection (7) I219-LM
- **Physical Address**: 8C-04-BA-02-65-AB
- **DHCP Enabled**: Yes
- **Autoconfiguration Enabled**: Yes
- **Link-local IPv6 Address**: fe80::4846:20a3:30f1:2a97%11 (Preferred)
- **IPv4 Address**: 192.168.1.100 (Preferred)
- **Subnet Mask**: 255.255.255.0
- **Lease Obtained**: Sunday, November 10, 2019 3:35:10 PM
- **Lease Expires**: Monday, November 11, 2019 3:40:25 PM
- **Default Gateway**: 192.168.1.1
- **DHCP Server**: 192.168.1.1
- **DHCPv6 IAID**: 126616762
- **DHCPv6 Client DUID**: 00-01-00-01-24-FC-97-A1-8C-04-BA-02-65-AB
- **DNS Servers**: 192.168.2.1
- **NetBIOS over Tcpip**: Enabled

If the PC is connected to WiFi, the DNS server will display in this section:

**Wireless LAN adapter Wi-Fi:**

- **Connection-specific DNS Suffix**: Qualcomm QCA61x4A 802.11ac Wireless Adapter
- **Physical Address**: EC-5C-68-78-04-5F
- **DHCP Enabled**: Yes
- **Autoconfiguration Enabled**: Yes
- **Link-local IPv6 Address**: fe80::355f:cf49:3a1f:b745%6 (Preferred)
- **IPv4 Address**: 192.168.1.101 (Preferred)
- **Subnet Mask**: 255.255.255.0
- **Lease Obtained**: Sunday, November 10, 2019 12:31:55 PM
- **Lease Expires**: Monday, November 11, 2019 12:31:56 PM
- **Default Gateway**: 192.168.1.1
- **DHCP Server**: 192.168.1.1
- **DHCPv6 IAID**: 267148392
- **DHCPv6 Client DUID**: 00-01-00-01-24-FC-97-A1-8C-04-BA-02-65-AB
- **DNS Servers**: 192.168.2.1
- **NetBIOS over Tcpip**: Enabled
If using a MAC computer, `scutil --dns` Terminal command displays the Linksys local DNS server 192.168.2.1 instead of the MalBlock servers:

```
DNS configuration (for scoped queries)

resolver #1
  nameserver[0] : 192.168.2.1
  if_index : 8 (en0)
  flags : Scoped, Request A records
  reach : 0x00020002 (Reachable,Directly Reachable Address)
```

*End of Document*