MalBlock Settings

Before you can configure MalBlock Settings, you must first login to MyAccount and open the MalBlock portal.

Access the MalBlock Portal

Use the following steps to login to MyAccount and access the MalBlock portal.

1. Enter coxbusiness.com in your web browser.
2. Click the Sign In MyAccount link at the top of the page.
3. Enter the User ID and Password. (Note: These values are provided in the email you received from Cox Business.)
   Result: The MyAccount Welcome page appears.
4. Scroll to the My Services section and click the Internet tab.
5. Click the MalBlock DNS Security icon.
   Result: The MalBlock DNS Security page displays. (See Figure 1.)

Figure 1. MalBlock DNS Security screen
Access Settings: Protection Preferences

The Protection Preferences screen allows you to configure Protection Levels, Off Hours Internet Schedule, Malware and Phishing Protection and Search Protection.

Use the following steps to access the MalBlock Settings Protection tab.

1. Login to the MalBlock portal.
2. Click the Malblock Dashboard button. 
   **Result:** The Usage Statistics page appears.
3. Click the Settings tab. 
   **Result:** The Settings screen appears and defaults to the Protection Preferences page. Devices and Block and Allow Lists tabs also appear. (See Figure 2.)

Figure 2. Settings: Protection Preferences screen

Refer to the table below for descriptions and instructions on the highlighted setting types shown in Figure 1.
<table>
<thead>
<tr>
<th>Heading</th>
<th>Description and Instructions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protection Level</td>
<td>Displays categories of content you want to allow and restrict. The example in Figure 2 displays a sample list of 32 Allowed and 26 Blocked groups. Blocked categories cannot be viewed.</td>
</tr>
<tr>
<td></td>
<td>Click the <strong>Allow</strong> ✓ or <strong>Block</strong> ✗ symbol at the left of the category to reclassify a category.</td>
</tr>
<tr>
<td></td>
<td>Slide the <strong>Content Restriction Schedule</strong>* toggle to <strong>ON</strong> to establish specific days and time periods you want to restrict certain categories. If you never want categories to be viewable, leave the toggle at the <strong>OFF</strong> position. (<em>For Administrators only.</em>)</td>
</tr>
<tr>
<td>Internet Off (Off-Hours Internet Schedule)</td>
<td>Slide the <strong>Off-Hours Internet Schedule</strong>* toggle to <strong>ON</strong> to create a rule that establishes specific days and time periods you want the Internet to be available to employees or guests. You can create multiple rules can based on your business requirements. (<em>For Administrators only.</em>)</td>
</tr>
<tr>
<td>Internet Security (Malware and Phishing Protection)</td>
<td>Slide the Malware and Phishing Protection toggle to <strong>ON</strong> to prevent users from infecting your network by inadvertently accessing affected webpages or clicking links within phishing emails.</td>
</tr>
<tr>
<td>Internet Security (Search Protection)</td>
<td>Check a web site box to filter search results.</td>
</tr>
</tbody>
</table>
Access Settings: Devices

When dnsmasq is enabled on your account, you can view or add devices on your company’s network. Administrators can sort devices, such as computers, into a customized group and set policies for that category based on company requirements. (Note: Groups can also be designated at the device level.)

Figure 3 displays two categories of devices: New Devices and Online Devices. Naming conventions can be customized to the most logical identification based on company requirements.

**Figure 3. Settings: Devices screen**

Use the following steps to view or add a new device.

1. Login to the MalBlock portal.
2. Click the **Malblock Dashboard** button
   **Result:** The Usage Statistics page appears.
3. Click the **Settings** tab.
   **Result:** The Settings screen appears.
4. Click the **Devices** tab.
   **Result:** A list appears with either New Devices that have not be saved (New Devices Unsaved) on the network and Online Devices that have not be assigned.
5. To add a new device, click the **Add Device** button in the upper right corner.
   **Result:** The Add Device dialog box appears.
6. Complete device registration by using the MAC address or the character code from the request. (Note: Click the **Where to find 4 character code** link for details.)
7. Click the **Add Device** button.
**Access Settings: Block and Allow Lists**

The Block and Allow Lists section allows administrators to designate specific websites that users can and cannot access regardless of the category defined in the Web Filters screen. (See Figure 2.) For example, in Figure 4, Facebook is accessible even though it falls within the otherwise blocked category of “Social Networking.”

**Figure 4. Settings: Block and Allow Lists screen**

Use the following steps to add or remove websites to Block and Allows Lists.

1. Login to the MalBlock portal.
2. Click the **Malblock Dashboard** button  
   **Result:** The Usage Statistics page appears.
3. Click the **Settings** tab.  
   **Result:** The Settings screen appears.
4. Click the **Block and Allows Lists** tab.  
   **Result:** A list of precise websites that are blocked or allowable appears.
5. To add a new website, enter the URL in the text field and click the **Check** button.  
   **Result:** A second screen appears that allows you to further identify whether you want to block or allow the whole website or the specific URL.
6. Click the **Block** or **Allow** button as appropriate.  
   **Result:** The website is added to the correct list.

*End of Document*