Overview

Cox Business MalBlock DNS Security ("MalBlock") is an in-depth defense, 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, gambling, violence, social media, and others.

MalBlock offers two levels of service: Standard and Premium and is easy to deploy and automatic if a customer inherits DNS server IP addresses via DHCP from Cox on their gateway or router. Otherwise some simple changes to the router's DNS and internal DHCP setting will get the service working.

⚠️ **Important:** MalBlock cannot clean or remove malware from a device already infected.

**Remediation** requires Endpoint Protection software (anti-virus/malware) such as McAfee, MalwareBytes, WebRoot, etc. to run a scan, quarantine and remove the malware.

**Ransomware** requires that the PC or server must be reimaged and restored from a backup.

This Quick Reference Guide includes steps for the following areas:

- How to log into MalBlock
- How to set a static IP address (for bring your own bandwidth users)
- How to view malware, phishing, and botnet activity
- How to navigate through the MalBlock Dashboard
How to Login to MalBlock

You can access MalBlock through the MyAccount portal.

**Figure 1. MyAccount Login screen**

1. Enter [myaccount.coxbusiness.com](http://myaccount.coxbusiness.com) in your web browser.
2. Enter your MyAccount **UserID** and **Password** and click the **Sign In** button. (See Figure 1.)
3. Scroll to the My Services section. **Note:** If there are multiple accounts, select the one with MalBlock service. If only one account exists, click the **Internet** tab and the **MalBlock DNS Security** icon to view the MalBlock Security screen.

**Figure 2. MyAccount Welcome screen**
If you are not in one of Cox Business’ franchise locations and are not being served by Cox’s Internet service, you need to 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.

If the device has a Static IP address, check the address for accuracy before you configure the remaining components of MalBlock. If your account does not have a static IP, check your device. If it fails, refer to the Administrator Guide.

You can find this information in the MalBlock Security screen and MalBlock IP Address Management screen. See the following page for instructions on how to add, view, or delete a static IP address.
Figure 4. **MalBlock IP Address Management screen**

Use the following steps to **add/view** a static IP address.

1. Login to MyAccount and click the **MalBlock DNS Security** icon.
2. Click the **Static IP address** button (see Figure 3). *(Note: If the business has one existing static IP address, the **Add IP Address** link appears in the MalBlock IP Address Management screen. See 0. However, if the business has multiple static IP addresses, MyAccount only displays two at a time and the **Add IP Address** link is no longer visible.)*

**Figure 5. Static IP Address table**

Use the following steps to **delete** a static IP address.

1. Login to MyAccount and click the **MalBlock DNS Security** icon.
2. Click the **Static IP address** button.
3. Click the trash can icon to the right of the IP address you want to remove.

**Malware, Phishing, and Botnet Protection**

Malware, Phishing, and Botnet Protection are included in MalBlock. The blocked counters in the dashboard update when the service blocks each type of threat. *(See 0 for links to both sections.)* Click either link to view the current status of Malware, Phishing, or Botnet activity.
Dashboard

The Dashboard page displays a summary of blocking history details for web filtering, malware, and botnets.

**Figure 6. MalBlock Dashboard screen**

Use the following steps to access the Dashboard.

1. Login to MyAccount and click the MalBlock DNS Security icon.
2. From the MalBlock Security Page, click the Dashboard button.
3. Use the date range drop-down menu to select the time range for which you want to see data. The options are 24 hours, 7 days, and 30 days.

Block and Allow Lists

The Block and Allow Lists function allows you to manually configure a specific URL you want to block or unblock.

**Figure 7. Block & Allow Lists screen**

Use the following steps to access the Block & Allow Lists screen.

1. Login to MyAccount and click the MalBlock DNS Security icon.
2. From the MalBlock Security Page, click the Dashboard button.
3. From the top toolbar, click the Block Page Customization link.
4. Enter the URL and click the **Check** button, then click the **Block** or **Allow** buttons to add the URL to the respective list.

5. To delete a URL from either list, click the **Remove** link to the right of the URL.

**Block Page Customization**

Customize the page and message that the user will see when they attempt to access blocked URLs. You can add branding to the page, add an explanation to the alert, and provide a contact of someone who can give more details or unblock access.

By default, the block page is minimal. It displays a short alert indicating the reason for blocking:

- **Global URL Filtering**: the content is blacklisted or belongs to a category that is blocked
- **Malware and Phishing** if the content poses the risk of malware or phishing

**Domain Lookup**

Find the web filter category to which a URL is assigned. (Available only with Premium.)

**Scheduled Reports**

Select Scheduled Reports to designate an email recipient and set a cadence for reports that show blocked threats and filtered content. You can set up usage report generation for daily, weekly, or monthly timeframes.

**Technical Support**

For help with technical issues, call 866-272-5777 or visit **coxbusiness.com/starhere**.