Comcast Xfinity Router Setup

Most Xfinity routers for both residential and business users come with the firmware that intercepts all DNS requests. Even if DNS addresses are changed, the router will continue redirecting DNS requests to Comcast servers.

Business users

For business users, DNS interception is controlled by the **Security Edge** feature that can be disabled in your account on the Comcast for Business portal.

Residential users

Unfortunately, residential users can not disable DNS interception on Xfinity routers.

However, there are several possible solutions on how to bypass DNS interception.

Solution 1 - connect a third-party router

Connecting a third-party router to Xfinity router will create a secondary network in which you have full control over router's settings. After that, set up the third-party router using this guide for routers and connect all your devices to it.

Solution 2 - install SafeDNS Agent on devices

> The Agent is available on the following billing plans: **Safe Family, Pro, Pro Plus,** and archived **Safe@Home, Safe@Office**.

Alternatively, you can install SafeDNS Agents on all devices that require filtering. SafeDNS Agent works in any network.

Windows, Mac, Linux, Android

If you have installed SafeDNS Agent and the filtering doesn't work correctly, please check the parental control feature:

1. Log into Xfinity dashboard.
2. Navigate to **Network**.
3. Select your gateway/router.
4. Select **device** you need to remove parental controls from.
   Unfortunately, this setting has to be disabled for each device separately.
5. Scroll down to the **Assigned to** panel and click on the cogwheel icon.
6. Click on the **parental control** option.
7. Select **Off** and click **Apply Changes**.

Solution 3 - use OpenVPN for filtering on devices

The filtering can be set up using a third-party application OpenVPN on all devices that require filtering.

Please follow this guide for OpenVPN setup.

Solution 4 - use DNS-over-HTTPS

Please follow this guide for DoH setup.