AT&T Business

AT&T DNS Security, AT&T DNS Security Advanced and Enterprise Traffic Protector (ETP) Configuration Guide

How to configure your DNS forwarders on your network devices to AT&T DNS Security servers

Contents

Welcome to AT&T DNS Security, AT&T DNS Security Advanced and Enterprise Traffic Protector (ETP) configuration guide

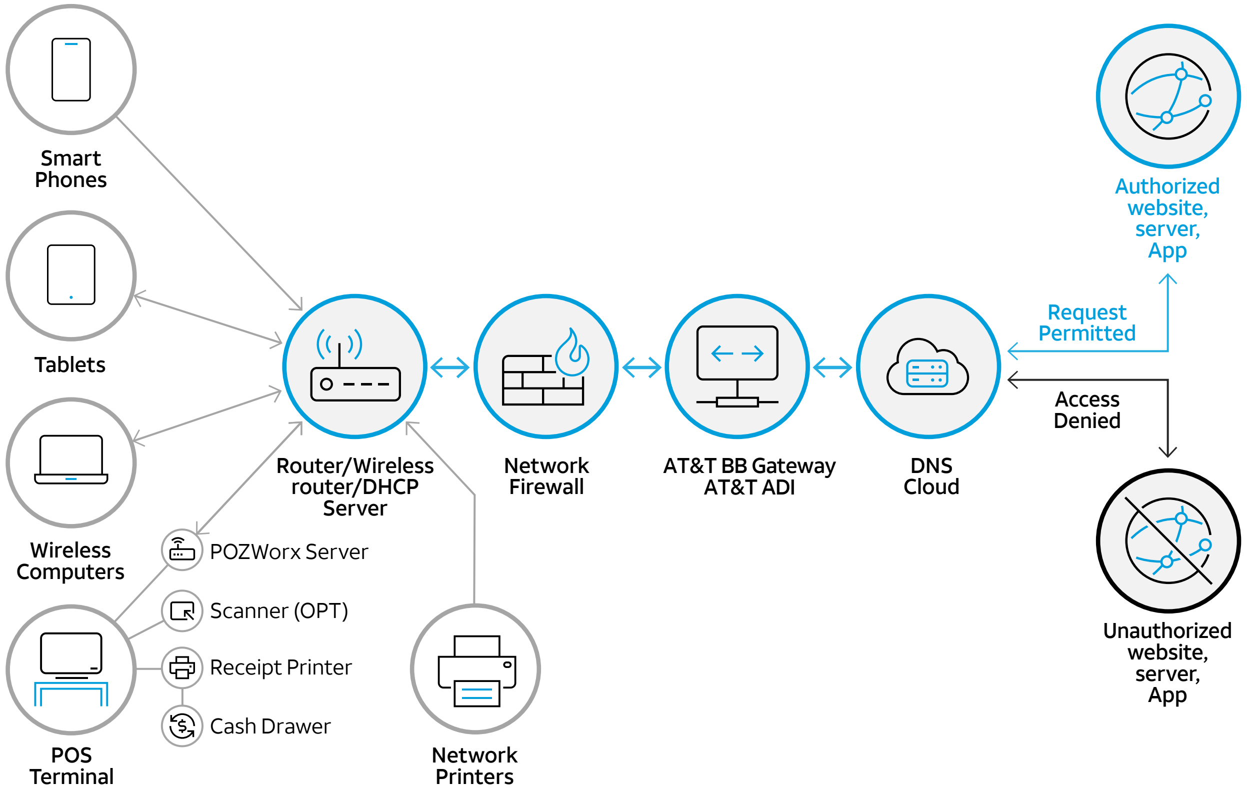
DNS Security, DNS Security Advanced, and ETP are cloud-based threat monitoring solutions for outbound internet traffic activity.
DNS Security provides threat intelligence reporting that identifies internet risks that your users may unknowingly expose your online operation to. DNS Security Advanced & ETP also provides threat intelligence reporting plus security protection that identifies and block threats such as malware, phishing, and data exfiltration before these risks impact your business.
This guide will help you take the simple steps to enable monitoring for DNS Security and monitoring and protection for DNS Security Advanced & ETP at the server or network firewall level.

How to use this document – what you need to do
This guide lists the various DHCP servers and firewalls that you may have for your business. Identify the name of your server or firewall or router and follow the steps listed in this document to forward DNS to the AT&T IP address provided on your order welcome email.

AT&T will provision DNS Security Advanced service for customers that have AT&T Broadband Gateway Router number: 2310/2210/NM55/RG2701/RG3600/RG3800/3801/iNID/5031NV/NVG510/5168NV/NVG589/NVG595/NVG599/5268AC/BGW210-700/BGW320-500/BGW320-505.

DNS Security and ETP customers will activate their respective servicer as per the welcome email received.

Where to change your DNS IP forwarding



NOTE: When you change the DNS IPs on the device level, you'll have to change the DNS IPs for every device. It's recommended that you forward the DNS IPs at the router / DHCP Server level or the network firewall level so that the configuration applies to all your devices.

Table of Contents

Configure DNS forwarders on Microsoft Windows Server 2008 R2 and 2016

Before you begin

Note your existing IP addresses and IP addresses of the AT&T DNS SECURITY DNS servers provided to you on your order welcome email.

Confirm that you have a root hints file configured. The root hints file contains the list of root DNS servers that Active Directory contacts for recursion.

Complete these procedures to configure DNS forwarding on the Microsoft Windows Server 2008 R2 and 2016. You can configure DNS forwarding with the Windows Server graphical user interface or the command line.

Graphical user interface

How to

1) Click **Start** and then **Administrative Tools**. Click **DNS**.
2) Right-click the DNS server that you want to configure as a forwarder.
3) In the **Action** menu, select **Properties**.
4) Click the **Forwarders** tab.
5) Click **Edit**.
6) In the **Edit Forwarders** dialog, enter the primary IP address of the AT&T DNS SECURITY recursive DNS server and press **Enter**.
7) Enter the secondary IP address of the AT&T DNS SECURITY recursive DNS server and press **Enter**.
8) If other servers are listed as forwarders, then remove them. The primary and secondary recursive DNS servers should be the only forwarders listed.
9) To change the number of seconds that a DNS server waits for a response before it tries the IP address of the other DNS server, enter a new value in the **Number of seconds before forward queries times out** field.
10) Click **OK**.
11) Enable the **Use roots hints if no forwarders are available** option. This option ensures that DNS servers in a root hints file resolve the name locally.
12) In the properties dialog, click **OK**.

Command line interface

How to

1) Open a command prompt. Run the command prompt as an administrator.
2) Type the below command and press **Enter:**

   ```
   dnscmd <ServerName> /ResetForwarders <PrimaryIPaddress ...> [/TimeOut <Time>] /noslave
   ```

   <ServerName> is the hostname or IP address of the DNS server. To specify the DNS on your local computer, you can type (.)

   <PrimaryIPaddress ...> is one or more IP addresses of the DNS servers where you are forwarding queries. In this case, enter the AT&T DNS SECURITY server IP addresses. Separate each IP address with a space.

   <Time> is the value that you want to configure for the time out setting in seconds. The default time out value is five seconds. For more information, see Microsoft documentation.

   Note: The /noslave parameter indicates that the server will use the root hints file to resolve requests locally if it cannot reach AT&T DNS SECURITY.

Table of Contents

Configure DNS forwarding on BIND

Before you begin

Note your existing IP addresses and IP addresses of the AT&T DNS SECURITY DNS servers provided to you on your order welcome email.

Complete this procedure to configure DNS forwarding on the BIND DNS server.

How to

1) Open a command prompt or terminal.
2) If you are using a Secure Shell (SSH), enter ssh username@server

   where:

   a) "username" is the username to access the server remotely.

   b) "server" is the hostname or IP address of the server.
3) Change the directory to **etc/bind**.
4) Open the **named.conf.options** file to edit it.
5) In the forwarders area, enter the IP addresses of the AT&T DNS SECURITY DNS servers.

   Make sure that you enter the IP addresses between the { } symbols.

   Note: If this BIND server is also a secondary authoritative server for internal zones and you do not want to forward these queries to AT&T DNS SECURITY, you can configure those zones with a blank forwarders list by adding forwarders {} to the internal zone settings in the configuration file. This ensures that recursion for subdomains occurs in the internal zone only.
6) **Save** and close the file.

Next steps

Restart the BIND daemon. In the terminal, enter this command:

```
sudo service bind9 restart
```

Table of Contents

Configure DNS forwarding on Blue Coat ProxySG

Before you begin

Note your existing IP addresses and IP addresses of the AT&T DNS SECURITY DNS servers provided to you on your order welcome email.

Complete this procedure to configure DNS Forwarding on Blue Coat ProxySG.

How to

1) In the ProxySG Management Console, click the **Configuration** tab.
2) In the navigation menu, click **Network > DNS**.
3) In the DNS fields, enter the primary and the secondary IP addresses of the AT&T DNS SECURITY recursive servers.
4) Click **Apply**.

Next

Complete these steps to perform a DNS resolution test:

1) Establish an SSH connection to the ProxySG appliance.
2) Enter this command and press **Enter**:

   ```
   SG>test dns <domain>
   ```

   <domain> is a domain you want to resolve for this test.

Table of
Contents

Configure a DNS proxy on a Palo Alto Networks firewall

Before you begin

Note your existing IP addresses and IP addresses of the AT&T DNS SECURITY DNS servers provided to you on your order welcome email.

Complete this procedure to configure a DNS proxy on a Palo Alto Networks firewall.

How to

1) In the Palo Alto Networks firewall, go to **Network > DNS Proxy**.
2) Click **Add**.
3) Select the interface or interfaces where the DNS proxy is enabled.
4) In the **Inheritance Source** list, select none.
5) In the **Primary** field, enter the primary IP address of the AT&T DNS SECURITY recursive server.
6) In the **Secondary** field, enter the secondary IP address of the AT&T DNS SECURITY recursive server.
7) To configure static DNS entries that are cached and resolved locally, in the **Static Entries** tab, click **Add** and:

    a. In the **Name** column, enter a name to identify the entry

    b. In the **FQDN** column, enter the **Fully Qualified Domain Name** that you want the firewall to resolve locally

    c. In the **Address** column, enter the associated IP address or addresses

8) To configure DNS caching, in the **Advanced** tab, select **Cache**. By default, the DNS proxy populates values for the cache size and timeout.
9) Click **OK**.

Table of Contents

Configure DNS recursion on Citrix NetScaler

Before you begin

Note your existing IP addresses and IP addresses of the AT&T DNS SECURITY DNS servers provided to you on your order welcome email.

Complete one of these procedures to configure a recursive DNS server on Citrix NetScaler. You can configure DNS recursion on the NetScaler graphical or command line interface.

Note: In NetScaler, DNS recursion applies to a local DNS server configuration only. This functionality is not available in an Authoritative Domain Name Server (ADNS) configuration.

Graphical user interface

How to

1) In the navigation menu, click **Traffic Management > DNS**.
2) Click **Change DNS Settings**.
3) In the **Change DNS Settings** dialog:
4) Select **Enable recursion**.
5) To enable caching, select **Records caching**.
6) Click **OK**.
7) In the expanded navigation menu for DNS, select **Name Servers**.
8) Click **Add**.
9) In the Create Name Server dialog:
10) Make sure that IP address is selected.
11) In the **IP Address** field, enter the IP address of the primary AT&T DNS SECURITY recursive server.
12) Select **Local**.
13) Click **Create**.
14) To add the secondary AT&T DNS SECURITY recursive server, repeat steps 5 and 6.
15) Repeat steps 5 and 6 to add a recursive DNS server that will resolve requests if NetScaler cannot reach AT&T DNS SECURITY.

Command line interface

How to

1) Establish an SSH connection to the NetScaler appliance.
2) To configure an AT&T DNS SECURITY DNS server as a DNS nameserver, enter this command and press **Enter**:

```
add dns nameserver <IP address> -local
```

3) where <IP address> is the IP address of the AT&T DNS SECURITY recursive DNS Server. To enable DNS recursion, enter this command and press **Enter**:

```
set dns parameter -recursion ENABLED -cacheRecords YES
```

4) Repeat step 2 to add a recursive DNS server that will resolve requests if NetScaler cannot reach AT&T DNS SECURITY.

Table of Contents

Configure DNS forwarders on Linksys Routers

Before you begin

Note your existing IP addresses and IP addresses of the AT&T DNS SECURITY DNS servers provided to you on your order welcome email.

Complete this procedure to configure DNS Forwarding on Linksys Routers.

How to

1) Sign into your Linksys router's web-based administration, usually at the following address:

   http://192.168.1.1

2) Select **Setup** in the top menu.
3) Select **Basic Setup** in the **Setup** submenu.
4) In the **Static DNS 1** field, enter the primary DNS server you want to use. You need to enter at least one DNS address.
5) In the **Static DNS 2** field, enter the secondary DNS server you want to use.
6) Leave the **Static DNS 3** field blank or add a primary DNS server from another provider.
7) Select **Apply** at the bottom of the screen.

Most Linksys routers don't require a restart for these DNS server changes to take effect, but if the router admin page asks you to, do it.

See this Linksys default password list if 192.168.1.1 doesn't work for you. Not all Linksys routers use this address.

Linksys makes small changes to its administration page every time the company releases a new series of routers. If the procedure above doesn't work for you, the instructions you need are in the router manual, which you can get at Linksys' site.

Table of Contents

Configure DNS forwarders on NetGear Router

Before you begin

Note your existing IP addresses and IP addresses of the AT&T DNS SECURITY DNS servers provided to you on your order welcome email.

Complete this procedure to configure DNS Forwarding on NetGear Routers.

How to

Change the DNS servers on your NetGear router from the Basic Settings or Internet menu, depending on your model.

1) Sign into your NetGear router manager page, most often by entering

   http://192.168.1.1

   or

   http://192.168.0.1

   in a web browser.

2) NetGear has two primary interfaces with different ways to perform the next step: If you see **Basic** and **Advanced** tabs along the top, choose **Basic**, followed by the **Internet** option on the left. If you don't have those two tabs along the top, choose **Basic Settings**.
3) Choose the **Use These DNS Servers** option in the **Domain Name Server (DNS) Address** section.
4) In the **Primary DNS** field, enter the primary DNS server you want to use.
5) In the **Secondary DNS** field, enter the secondary DNS server you want to use.
6) Select **Apply** to save the DNS server changes you just entered.
7) Follow any additional prompts about restarting the router. If you don't get any additional prompts, your changes should now be live.

NETGEAR routers have used several default gateway addresses over the years, so if 192.168.0.1 or 192.168.1.1 doesn't work for you, find your model in this NETGEAR default password list.

While this process works with most NETGEAR routers, there may be a model or two that use a different method. Visit NETGEAR's support site to find the PDF manual for your specific model, which contains the instructions you need.

Table of Contents

Configure DNS forwarders on D-Link Router in the Setup menu

Before you begin

Note your existing IP addresses and IP addresses of the AT&T DNS SECURITY DNS servers provided to you on your order welcome email.

Complete this procedure to configure DNS Forwarding on D-Link Router.

How to

1) Sign into your D-Link router with a web browser using

   http://192.168.0.1

2) Choose the **Internet** option on the left side of the page.
3) Select the **Setup** menu at the top of the page.
4) Find the **Dynamic IP (DHCP) Internet Connection Type** section and enter the primary DNS server you want to use into the **Primary DNS Address** field.
5) In the **Secondary DNS Address** field, enter the secondary DNS server you want to use.
6) Choose the **Save Settings** button at the top of the page.
7) The DNS server settings should have changed instantly, but you might be prompted to reboot the router to complete the changes.

While you can access most D-Link routers via 192.168.0.1, a few models use a different default. If that address doesn't work for you, see the D-Link default password list to find your specific model's default IP address and the default password for logging on.

If the process above doesn't seem to apply for you, see the D-Link support page for information on finding the product manual for your specific D-Link router.

Table of Contents

Configure DNS forwarders on Asus Router through the LAN menu

Before you begin

Note your existing IP addresses and IP addresses of the AT&T DNS SECURITY DNS servers provided to you on your order welcome email.

Complete this procedure to configure DNS Forwarding on Asus Routers.

How to

1) Sign into your Asus router's admin page with this address

    http://192.168.1.1

2) From the menu on the left, select **LAN** or **WAN**.
3) Choose the **Internet Connection** tab at the top of the page.
4) In the **WAN DNS Setting** section, enter the primary DNS server you want to use in the **DNS Server1** text box.
5) Enter the secondary DNS server you want to use in the **DNS Server2** text box if desired. You need to enter at least one DNS address.
6) Save the changes with the **Apply** button at the bottom of the page. You may need to restart the router after applying the changes.

You should be able to access the configuration page for most Asus routers with the 192.168.1.1 address. If you never changed your sign-in information, use **admin** for both the username and the password.

The software on every Asus router isn't the same. If you can't get into your router's configuration page using the steps described here, find the router manual with specific instructions on the Asus support website.

Table of Contents

Configure DNS forwarders on TP-LINK router via the DHCP menu

Before you begin

Note your existing IP addresses and IP addresses of the AT&T DNS SECURITY DNS servers provided to you on your order welcome email.

Complete this procedure to configure DNS Forwarding on TP-LINK Routers.

How to

1) Sign into your TP-LINK router's configuration page, usually via this address:

   http://192.168.1.1

   or this one:

   http://192.168.0.1

2) Select **Network** in the left pane. Select **WAN** under Network. Select the **Use These DNS Servers** check box. Enter the DNS server for AT&T DNS Security. Choose the **Save** button at the bottom of the page to save the changes. You may not have to restart the router to apply these DNS settings, but some TP-LINK routers require it.

One of the two IP addresses used in this tutorial should work for most TP-LINK routers. If not, search for your TP-LINK model at the TP-LINK support page. Your router's manual provides the default IP you should use to connect, as well as details on the DNS-change procedure.

Table of
Contents

Configure DNS forwarders on a Cisco Router from the LAN Setup menu

Before you begin

Note your existing IP addresses and IP addresses of the AT&T DNS SECURITY DNS servers provided to you on your order welcome email.

Complete this procedure to configure DNS Forwarding on Cisco.

How to

1) Sign into your Cisco router using either:

   http://192.168.1.1

   or

   http://192.168.1.254

   depending on the router model.
2) Select **Setup** on the menu at the top of the page.
3) Select the **Lan Setup** tab from the menu that's just below the **Setup** option.
4) In the **LAN 1 Static DNS 1** field, enter the primary DNS server you want to use.
5) In the **LAN 1 Static DNS 2** field, enter the secondary DNS server you want to use if desired. Some Cisco routers may have a **LAN 1 Static DNS 3** field. You can leave it blank or enter another DNS server.
6) Save the changes using the **Save Settings** button at the bottom of the page. On some Cisco routers, you may need to restart the router to apply the changes.

Having trouble with the directions? Visit Cisco's support site to find the manual for your specific Cisco router model. Some models require different steps to reach the DNS server settings, but the manual for your specific router is correct for your model.

If you can't open the Cisco router's configuration page using one of the default addresses, look through this Cisco default password list for the default IP address, along with other default login data for your Cisco router.

These steps are different for your router if you have a co-branded Cisco-Linksys router. If your router has the word Linksys on it anywhere, follow the steps at the top of this article for changing the DNS servers on a Linksys router.

Table of Contents

Configure DNS forwarders on a TRENDnet Router via the Advanced menu

Before you begin

Note your existing IP addresses and IP addresses of the AT&T DNS SECURITY DNS servers provided to you on your order welcome email.

Complete this procedure to configure DNS Forwarding on TRENDnet.

How to

1) Sign into your TRENDnet router at

   http://192.168.10.1

2) Choose **Advanced** at the top of the page.
3) Select the **Setup** menu to the left.
4) Select the **Internet settings** submenu under the **Setup** menu.
5) Choose the **Enable** option next to **Manually configure DNS**.
6) Next to the **Primary DNS** box, enter the primary DNS server you want to use.
7) Use the **Secondary DNS** field if there is a secondary DNS server you want to use.
8) Save the settings with the **Apply** button.
9) If you're told to reboot the router, follow the instructions on the screen. Not all TRENDnet models require this.

These instructions should work for most TRENDnet routers. If these instructions don't work, go to the TRENDnet support page and look for the PDF user guide for your model.

Table of Contents

Configure DNS forwarders on a Belkin Router by opening the DNS menu

Before you begin

Note your existing IP addresses and IP addresses of the AT&T DNS SECURITY DNS servers provided to you on your order welcome email.

Complete this procedure to configure DNS Forwarding on Belkin Routers.

How to

1) Sign into your Belkin router through this address:

   http://192.168.2.1

2) Select **DDNS** under **Advanced Settings > Firewall**.
3) In the **DNS Address** field, enter the primary DNS server you want to use.
4) In the **Secondary DNS Address** field, enter the secondary DNS server if you'd like to use one.
5) Select **Apply Changes** to save the changes.
6) You might be told to restart the router for the changes to take effect. If so, follow the on-screen prompts.

You can reach nearly all Belkin routers with 192.168.2.1, but there are exceptions where a different address is used by default. If this IP address doesn't work for you, the specific one you should use with your model can be found on the Belkin support page.

Table of
Contents

Configure DNS forwarders on a Buffalo Router from the Advanced menu

Before you begin

Note your existing IP addresses and IP addresses of the AT&T DNS SECURITY ADVANCED DNS servers provided to you on your order welcome email.

Complete this procedure to configure DNS Forwarding on Buffalo Router.

How to

1) Sign into your Buffalo router at

   http://192.168.11.1

2) Select the **Advanced** tab at the top of the page.
3) Choose **WAN Config** on the left side of the page.
4) Next to the **Primary field** in the **Advanced Settings** section, enter the primary DNS server.
5) Next to the **Secondary** field, type the secondary DNS server you want to use.
6) Near the bottom of the page, choose **Apply** to save the changes.

If the administration IP address isn't working, or the other steps don't seem right for your Buffalo router model, find specific instructions in your router's user manual, available from the Buffalo support page.

Table of Contents

Configure DNS forwarders on Google Wi-Fi Router from Advanced networking menu

Before you begin

Note your existing IP addresses and IP addresses of the AT&T DNS SECURITY DNS servers provided to you on your order welcome email.

Complete this procedure to configure DNS Forwarding on Buffalo Router.

How to

1) Open the Google Wi-Fi app on your mobile device. You can download the Google Wi-Fi app from the Google Play Store for Android or the Apple App Store for iOS devices.
2) Select the upper-right menu item to enter the settings.
3) Scroll down to the **Settings** section and choose **Network & General**.
4) Tap **Advanced networking** in the **Network** section.
5) Choose the **DNS** item.

   Google Wi-Fi uses Google's DNS servers by default, but you have the option to change the servers to your ISP's or a custom set.
6) Select **Custom** to find two new text boxes.
7) Next to the **Primary server** text field, enter the DNS server you want to use with Google Wi-Fi.
8) Next to **Secondary server**, enter an optional secondary DNS server.
9) Select the **Save** button at the upper-right corner of the Google Wi-Fi app.

Unlike routers from other manufacturers, you cannot access Google Wi-Fi settings from your computer using its IP address. You must use the accompanying mobile app.

All the Google Wi-Fi mesh points connected to one network use the same DNS servers that you choose following the steps above. You can't pick different DNS servers for each Wi-Fi point.

If you need additional help, consult the Google Wi-Fi help center for more information.

Table of Contents

Configure DNS forwarders on MAC OS

Before you begin

Note your existing IP addresses and IP addresses of the AT&T DNS SECURITY ADVANCED DNS servers provided to you on your order welcome email.

Complete this procedure to configure DNS Forwarding on MAC OS.

How to

1) Go to the Apple menu and select **System Preferences**
2) Choose the **Network** control panel
3) Select your network interface from the left side ("Wi-Fi" or "Ethernet" for example)
4) Click the **Advanced** button in the lower right corner of the Network window.
5) Choose the **DNS** tab at the top of the screen to edit, add, or remove DNS
    a. To add new AT&T DNS Security Service servers: click on the **[+] plus** button.
    b. To edit an existing DNS server: **click twice on the DNS IP address** you wish to change.
    c. To remove a DNS server: select a DNS server IP address and then click either the **[-] minus** button **OR** the **delete** key
6) When finished making changes to the DNS settings, click the **OK** button.
7) Now click **Apply** for the DNS changes to take effect, and close out of System Preferences as usual.

Table of
Contents

Configure DNS forwarders on Windows 10 using Control Panel

Before you begin

Note your existing IP addresses and IP addresses of the AT&T DNS SECURITY ADVANCED DNS servers provided to you on your order welcome email.

Complete this procedure to configure DNS Forwarding on **Windows 10**.

How To

1) Open **Control Panel**.
2) Click on **Network** and **Internet**.
3) Click on **Network** and **Sharing Center**.
4) Click the **Change adapter settings** option in the left pane
5) Right-click the network interface that connects Windows 10 to the internet and select the Properties option. **Quick tip:** You'll know which adapter is connected to the network, because it will not have a "Disabled" or "Network cable unplugged" label.
6) Select and check the **Internet Protocol Version 4 (TCP/IPv4)** option.
7) Click **Properties**.
8) Select the **Use the following DNS server addresses** option. **Quick note:** When you select the option to specify the DNS settings manually, the device will continue to receive the TCP/IP address from the DHCP server (router).
9) Type your **"preferred"** and **"alternate"** DNS addresses.
10) **Add** AT&T DNS Security Servers.
11) (Optional) Click the **Advanced** button.
12) Click the **DNS** tab.
13) Click **Add**.
14) Specify the alternate DNS server address.
15) Click **Add**. **Quick tip:** In addition to adding more addresses from this tab, you can also edit and remove resolvers, and you even have an option on the side to change their priorities.
16) Click **OK**.
17) Click **Close**.

Once you complete the steps, the device will immediately start using the DNS settings that you specified.

Table of
Contents

Configure DNS forwarders on Windows 10 using Settings

Before you begin

Note your existing IP addresses and IP addresses of the AT&T DNS SECURITY ADVANCED DNS servers provided to you on your order welcome email.

Complete this procedure to configure DNS Forwarding on **Windows 10**.

How To

1) Open **Settings**.
2) Click on **Network** and **Internet**.
3) Click on Ethernet (or Wi-Fi depending on your connection).
4) Select the connection that connects Windows 10 to the network.
5) Under the **IP settings** section, click Edit.
6) Use the **Edit IP settings** drop-down menu and select the **Manual** option.
7) Turn on the **IPv4** toggle switch.
8) Confirm your **“preferred”** and **“alternate”** DNS addresses. **Add** AT&T DNS Security Service DNS.
9) Click **Save**.

After you complete the steps, you should now be able to connect to the internet using the new resolvers.

Table of
Contents

Configure DNS forwarders on Chrome OS

Before you begin

Note your existing IP addresses and IP addresses of the AT&T DNS SECURITY ADVANCED DNS servers provided to you on your order welcome email.

Complete this procedure to configure DNS Forwarding on **Chrome OS**.

How to

1) Open the **Settings** screen on your Chrome OS device OR you can perform this function in a browser by opening the main menu, and then clicking the **Settings** option, OR you can also click your notification tray, and then click the gear-shaped **Settings** icon.
2) Click the **Wi-Fi** option under **Network** at the top of the **Settings** screen.
3) Click the name of the Wi-Fi network to which you're currently connected to change its settings.
4) Click to expand the **Network** section, locate the **Name Servers** option at the bottom of the expanded Network section, and then click the dropdown menu to its right.
5) Select **Custom name servers** to provide AT&T DNS Security server addresses.
6) Enter the primary and secondary AT&T DNS Security server addresses on their own separate lines.
7) Once you've typed the IP addresses, be sure to either press **Tab** or click outside the text field after typing the second address. If you close the window while typing the second IP address, it saves only the first IP address and not the second one. When you've performed this function, you can close the window.

Table of Contents