DNSFilter

Getting Started with DNSFilter

Navigating your onboarding experience

Welcome to DNSFilter's Customer Roadmap and Checklists! We're excited to guide you through the setup and optimization of your DNSFilter experience. Our comprehensive checklists are designed to ensure a smooth onboarding process and help you maximize the benefits of our service. Whether you're new to DNSFilter or looking to enhance your current setup, you'll find valuable resources and step-by-step instructions to help you every step of the way.

As you are getting started, we have provided individual checklists for each deployment type available to you:

1

Network Forwarding

- Our baseline deployment method allowing you to establish a blanket policy across your entire network at the router, firewall, DHCP level, and more
- Begin your Network Deployment

2

Roaming Clients

- Get user-level and device-level insights with our endpoint deployment method, expanding your policy assignment abilities
- Begin your Roaming Client Deployment

3

Relays

- Get per IP statistics via in-app generated or manual configuration options in alignment with VM, Docker, or OS focused install instructions
- Begin your Relay Deployment

Connect with us!

Explore our **Knowledge Base** for immediate access to helpful resources, and **join our growing Community** to connect with fellow DNSFilter users for questions, assistance, and engaging discussions!

DNSFilter

Getting Started with DNSFilter

Navigating your Deployment with Network Forwarding

We've prepared this Network Forwarding checklist to ensure a smooth transition and maximize the benefits of our platform. Start by reviewing the detailed sections of this checklist and completing each step in sequence! You can access both the checklist and your get-started instructions in our Knowledge Base at any time.

🏁 🏁 🏁

To get started, we recommend preparing your network for deployment

There are a few common issues that you can prevent before enabling DNS forwarding:

- Check that your Internet Service Provider (ISP) is not transparent proxying DNS traffic or using Carrier-Grade NAT
- Your environment is free of conflicting software or hardware settings:
  - Confirm any existing firewall, VPN, and security application rules or settings are set to allow traffic to the correct IP addresses
  - Prevent users from circumventing filtering policies
- Ensure all IP addresses, including primary external ones, secondary addresses from another ISP, and failover WAN links, are accounted for

1

☐ **Customize your first Filtering Policy**

- We provide a baseline recommendation for blocked categories as a starting place for all organizations
- Learn how to setup your Filtering Policy

2

☐ **Customize your first Block Page**

- This is the page your users see when they attempt to visit a domain that is not allowed according to your Filtering Policy
- Learn how to setup your Block Page

3

☐ **Setup your Site**

- Adding a Site to your network is the first step in protecting your network with your newly created Filtering Policy
- Learn how to add your Site

Connect with us!

Explore our **Knowledge Base** for immediate access to helpful resources, and **join our growing Community** to connect with fellow DNSFilter users for questions, assistance, and engaging discussions!

4

☐ Test your connection

- It is recommended to test your policy settings and check for conflicts for 1-2 days. Then, you can feel confident rolling out these policies at scale
- Learn how to test your connection

5

☐ Configure DNS Forwarding on your network

- Below are the most common configurations and use cases, but it is up to you which option is most preferable for your environment
- Explore DNSFilter Network Forwarding options

Router	• This is a common setup for smaller locations such as small or home offices, personal use, or locations without Local Authentications (e.g. Entra ID, LDAP, Radius, etc.) • Setup your router by searching "how to change DNS on ***Your ISP's Name***"
DHCP Server	• Ideal for utilizing NAT IPs, which allows for multiple filtering policies that correspond to network subnets ◦ This setup is best for Public/Guest Wi-Fi, No LAN resources, or utilizing the NAT IPs feature

Firewall	• Set as a standalone configuration to force query traffic or in concert with router/DHCP options.
	  ◦ Useful in scenarios where users may attempt to circumvent filtering
	  ◦ Also, if your ISP is running a transparent proxy to forward queries to port 5353 or 5354 (UDP only).

Congratulations!

You've successfully completed the DNSFilter New Customer Roadmap. Next, walkthrough your environment to get familiar with the dashboard and all reporting features!

You can review the integrations and resources available below to continue familiarizing yourself with DNSFilter:

Helpful insights

- Explore reporting through the different types of data visualization and evaluate DNS traffic
- Follow these instructions for mass deployment on Windows and macOS devices

Optional integrations

- Zapier: Connects you to over 3,000 popular applications to transfer data, trigger alerts, record activities, and integrate DNSFilter into normal business processes
- SIEM/Data Export, incl. Microsoft Sentinel: Export options that allow you to combine query log data with other data for monitoring, action, and alerting

Additional troubleshooting tips

- Websites aren't loading correctly:
  - The website is on the Allow List, but it's category is blocked
  - A site that should be allowed under my policy is blocked
- Visit our all-encompassing troubleshooting article for support with issues you're experiencing

Connect with us!

Explore our **Knowledge Base** for immediate access to helpful resources, and **join our growing Community** to connect with fellow DNSFilter users for questions, assistance, and engaging discussions!

DNSFilter

Getting Started with DNSFilter

Navigating your Deployment with Roaming Clients

We've prepared this Roaming Client checklist to ensure a smooth transition and maximize the benefits of our platform. Start by reviewing the detailed sections of this checklist and completing each step in sequence! You can access both the checklist and your get-started instructions in our Knowledge Base at any time.

🏁 🏁 🏁

To get started, we recommend preparing your device(s) for deployment

Environment cleanliness and application settings to review before enabling DNS forwarding:

- Clear browser and Operating System cache before installing Roaming Clients
- Your environment is free of conflicting software or hardware settings:
  - VPNs are set to allow DNS traffic to reach DNSFilter
  - Prevent end users from circumventing filtering policies
  - Set firewall settings to allow EDNS traffic (follow these guides for Windows or macOS devices)
- *Optional* Prepare your Local Domains for hotel and airline Captive Portals

1

☐ **Customize your first Filtering Policy**

- We provide a baseline recommendation for blocked categories as a starting place for all organizations
- Learn how to setup your Filtering Policy

2

☐ **Customize your first Block Page**

- This is the page your users will see when attempting to visit a domain that is not allowed according to your Filtering Policy
- Learn how to setup your Block Page

3

☐ **Setup your Site**

- Adding a Site is the first step in protecting your network with your newly created Filtering Policy
- Learn how to add your Site

Connect with us!

Explore our **Knowledge Base** for immediate access to helpful resources, and **join our growing Community** to connect with fellow DNSFilter users for questions, assistance, and engaging discussions!

4

☐ Select your Roaming Client type(s)

- Below you will find preparatory steps for each device with additional requirements
- Explore DNSFilter Roaming Client options

macOS	• Preparing your **macOS** Roaming Client
	  ◦ Other software is using the listener address and port
	  ◦ Update device settings to not block DNS traffic to DNSFilter
	• Setup your macOS Roaming Client

Windows	• Preparing your **Windows** Roaming Client
	  ◦ Machine has a WMI 'ExecQuery' failed message and install failed
	  ◦ It cannot bind to the correct port
	  ◦ There's limited internet connectivity once installed and online
	• Setup your Windows Roaming Client

Chromebook	• Apply customizable filtering policies based on IP or subnet, ensuring protection for devices where Roaming Client installation is unavailable, and receive per-machine reporting • Setup Chrome Extension Roaming Client

5

☐ Test your connection

- After your initial deployment setup, it is recommended to test your policy settings and check for conflicts for 1-2 days. Then you can feel confident rolling out these policies at scale
- Learn how to test your connection

Congratulations!

You've successfully completed the DNSFilter New Customer Roadmap. Next, walkthrough your environment to get familiar with the dashboard and all reporting features!

You can review the integrations and resources available below to continue familiarizing yourself with DNSFilter:

Helpful insights

- Explore reporting through the different types of data visualization and evaluate DNS traffic
- Follow these instructions for mass deployment on Windows and macOS devices

Optional integrations

- Zapier: Connects you to over 3,000 popular applications to transfer data, trigger alerts, record activities, and integrate DNSFilter into normal business processes
- Entra ID aka Active Directory: Synchronize DNSFilter user account creation and provisioning with existing deployments to apply specific policies, schedules, and block pages
- SIEM/Data Export, incl. Microsoft Sentinel: Export options that allow you to combine query log data with other data for monitoring, action, and alerting

Additional troubleshooting tips

- Local domain resolution failed while using the Windows or macOS Roaming Client
- The iOS Roaming Client shows up as "localhost" in the DNSFilter dashboard
- Visit our all-encompassing troubleshooting article for support with issues you're experiencing

Connect with us!

Explore our **Knowledge Base** for immediate access to helpful resources, and **join our growing Community** to connect with fellow DNSFilter users for questions, assistance, and engaging discussions!

DNSFilter

Getting Started with DNSFilter

Navigating your Deployment with Relays

We've prepared this Relay checklist to ensure a smooth transition and maximize the benefits of our platform. Start by reviewing the detailed sections of this checklist and completing each step in sequence! You can access both the checklist and your get-started instructions in our Knowledge Base at any time.

🏁 🏁 🏁

To get started, we recommend preparing your environment for deployment

There are a few common issues that you can prevent before enabling DNS forwarding:

- Your environment is free of conflicting software or hardware settings:
  - Confirm any existing firewall, VPN, and security application rules or settings are set to allow traffic to the correct IP addresses
  - Prevent users from circumventing filtering policies
- Ensure all IP addresses, including primary external ones, secondary addresses from another ISP, and failover WAN links, are accounted for

1

☐ **Customize your first Filtering Policy**

- We provide a baseline recommendation for blocked categories as a starting place for all organizations
- Learn how to setup your Filtering Policy

2

☐ **Customize your first Block Page**

- This is the page your users will see when attempting to visit a domain that is not allowed according to your Filtering Policy
- Learn how to setup your Block Page

3

☐ **Setup your Site**

- Adding a Site is the first step in protecting your network with your newly created Filtering Policy
- Learn how to add your Site

Connect with us!

Explore our **Knowledge Base** for immediate access to helpful resources, and **join our growing Community** to connect with fellow DNSFilter users for questions, assistance, and engaging discussions!

4

Generate your config.file for install

- The following link outlines the generated and manual config.file deployment options for installation as well as in-app download options for OS and binaries
- Explore DNSFilter Relay options

5

Test your connection

- It is recommended to test the connection with this nslookup command in the Virtual Machine or another device on the network for 1-2 days. Then you can feel confident rolling out these policies at scale
- Learn how to test your connection

Virtual Machine	nslookup -type=txt debug.dnsfilter.com 127.0.0.1
Network Device	nslookup -type=txt debug.dnsfilter.com <internal IP address>

Congratulations!

You've successfully completed the DNSFilter New Customer Roadmap. Next, walkthrough your environment to get familiar with the dashboard and all reporting features!

You can review the integrations and resources available below to continue familiarizing yourself with DNSFilter:

Helpful insights

- Explore reporting through the different types of data visualization and evaluate DNS traffic
- Deploy via Virtual Machine (VM) or Docker container when available to easily keep the Relay up to date

Optional integrations

- Zapier: Connects you to over 3,000 popular applications to transfer data, trigger alerts, record activities, and integrate DNSFilter into normal business processes
- SIEM/Data Export, incl. Microsoft Sentinel: Export options that allow you to combine query log data with other data for monitoring, action, and alerting

Additional troubleshooting tips

- Apple devices or the Safari browser are having difficulties loading websites
- Your deployment isn't auto-updating as expected or it's returning a bad output
- Visit our all-encompassing troubleshooting article for support with issues you're experiencing

Connect with us!

Explore our **Knowledge Base** for immediate access to helpful resources, and **join our growing Community** to connect with fellow DNSFilter users for questions, assistance, and engaging discussions!