Configuration, Filtering Policies, and Reporting

Frequently asked questions

Q. How easy is N-able™ DNS Filtering to configure?

It is very simple to set up. You need to be on **N-central® 2021.1 HF6** in order to enable DNS Filtering. Follow these steps for the installation:

1. At the System or Service Organization level, navigate to Integrations › Integration Management
2. On the main page to the right, click Activate on the line that includes DNS Filtering
3. Once activation is complete, DNS Filtering will display
4. Click Manage to begin setting up DNS Filtering for your Customers and Sites

Q. Can I have multiple policies on the same network?

Yes. There are a few ways to do this. You can implement separate subnets on your network and have DHCP hand out different DNS addresses to each subnet (we call this NAT IPs). We also offer a DNS Filtering Relay software component/VM which you can use to specify different policies. Or you can set up one of our Roaming Clients on devices that you wish to have separate policies on.

Q. Can I set different policies for different times of the day or different days of the week?

Yes, we have Filtering Schedules that you can set through an easy-to-use calendar. You can set different policies to take place anytime you like and any day you like.

Q. What is the hierarchy in which users, devices, roaming clients, and sites take priority?

The order of priority is as follows:

1. User-applied policy
2. Managed or Manual Collection
3. MAC address
4. Private IP address
5. Roaming Client
6. Site configured public IPs
7. Fallback DNS

Q. How responsive are you to recategorize sites?

In most cases, a submission to us is recategorized in 24-48 hours. You can always add the domain to your Allow list/Blocklist and changes take place immediately.

Q. What kind of reporting do you offer?

We have a reporting dashboard that allows you to filter timelines and per-site traffic in a variety of ways, so for all reports, you can view total aggregate or by a selection of sites. You can view request volume, categories, top requested domains, as well as threat reporting. This will show you which malicious domains were attempted by which locations, making it easy to see the security value in our product and also helping you to narrow down which sites may be infected and attempting to phone home.

Q. Do you offer multifactor authentication (MFA) or two-factor authentication (2FA) for account security?

Yes. Multifactor authentication is a way to secure your DNS Filtering account further by requiring more than just your username and password. You can set up multifactor authentication using any device capable of generating time-based, one-time password (TOTP) authentication codes, but we recommend using Google® Authenticator, Authy, 1Password, or LastPass authenticator.

Q. Should I use DNS over HTTPS?

The existence of DoH highlights the importance of maintaining control over your DNS data. By employing DNS Filtering to secure your DNS, you are preventing DNS tracking and spoofing. Instead of relying on your internet provider or any individual network, you are sending your traffic to a company that won't sell or manipulate your DNS data.

Q. Should I use DNS over TLS?

With Google (and Firefox®) adopting DoH as their DNS encryption method for their browsers, there seems to be a belief that DoH is superior to DoT. But that's not the case. The reality is that DNS-over-HTTPS and DNS-over-TLS are slightly different standards for implementing the same DNS protections. The main difference between DoT and DoH are the layers at which the encryption is enabled. DNS-over-HTTPS is applied at the application layer (two layers removed from the Internet layer) while DNS-over-TLS is applied at the transport layer (one layer removed from the Internet layer).

About N-able

N-able empowers managed services providers (MSPs) to help small and medium enterprises navigate the digital evolution. With a flexible technology platform and powerful integrations, we make it easy for MSPs to monitor, manage, and protect their end customer systems, data, and networks. Our growing portfolio of security, automation, and backup and recovery solutions is built for IT services management professionals. N-able simplifies complex ecosystems and enables customers to solve their most pressing challenges. We provide extensive, proactive support—through enriching partner programs, hands-on training, and growth resources—to help MSPs deliver exceptional value and achieve success at scale.